Defect Detection and Prevention (DDP): A Tool for Life Cycle Risk Management

Explanations, Demonstrations and Applications

Steve Cornford, Ph. D.

Strategic Systems Technology Program Office/

Safety and Mission Assurance Directorate

Jet Propulsion Laboratory,

California Institute of Technology

Phone:(818)354-1701, Email: steven.cornford@jpl.nasa.gov

GSFC
January 30, 2001

AGENDA

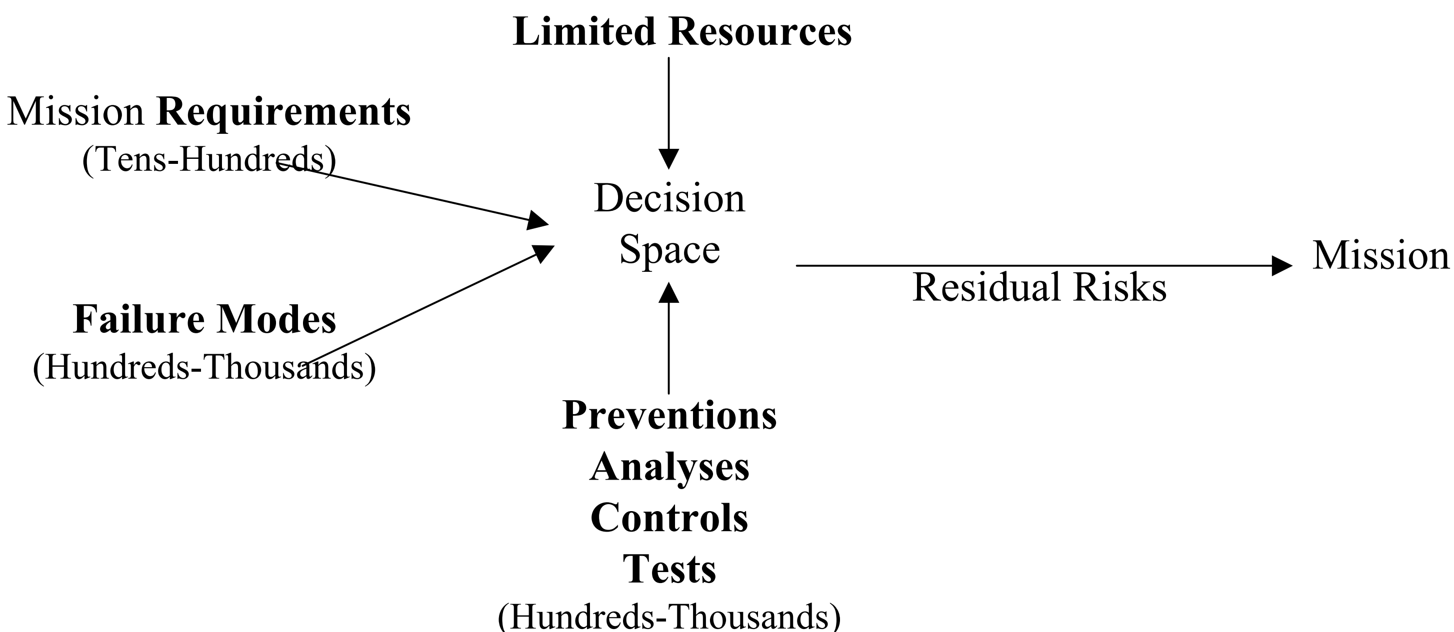
- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

BACKGROUND

- NASA's missions are challenging and "pushing the envelope"
- They may contain significant amounts of advanced technologies or existing technologies in advanced applications
- Risk Management
  - FBC + S! (Faster, Better, Cheaper and Safer)
  - "Risk as a resource" - Dr. Michael Greenfield, Code Q
  - NASA 7120.5, SMO, IPAO
- Team environment
  - Fast moving, implementation teams - need to integrate more extensive modeling/simulation results, need more accurate answers
  - Faster moving, formulation teams - need to integrate intuition and rapidly evolving designs, need 80% answer quickly
- Various resources are available
  - Advanced Design Environments/Tools
  - PRA, FMECA, DOORS, etc.

Challenge: Get the job done effectively and efficiently. We need a process/tool to enable life-cycle risk management.

Parameters in the Problem



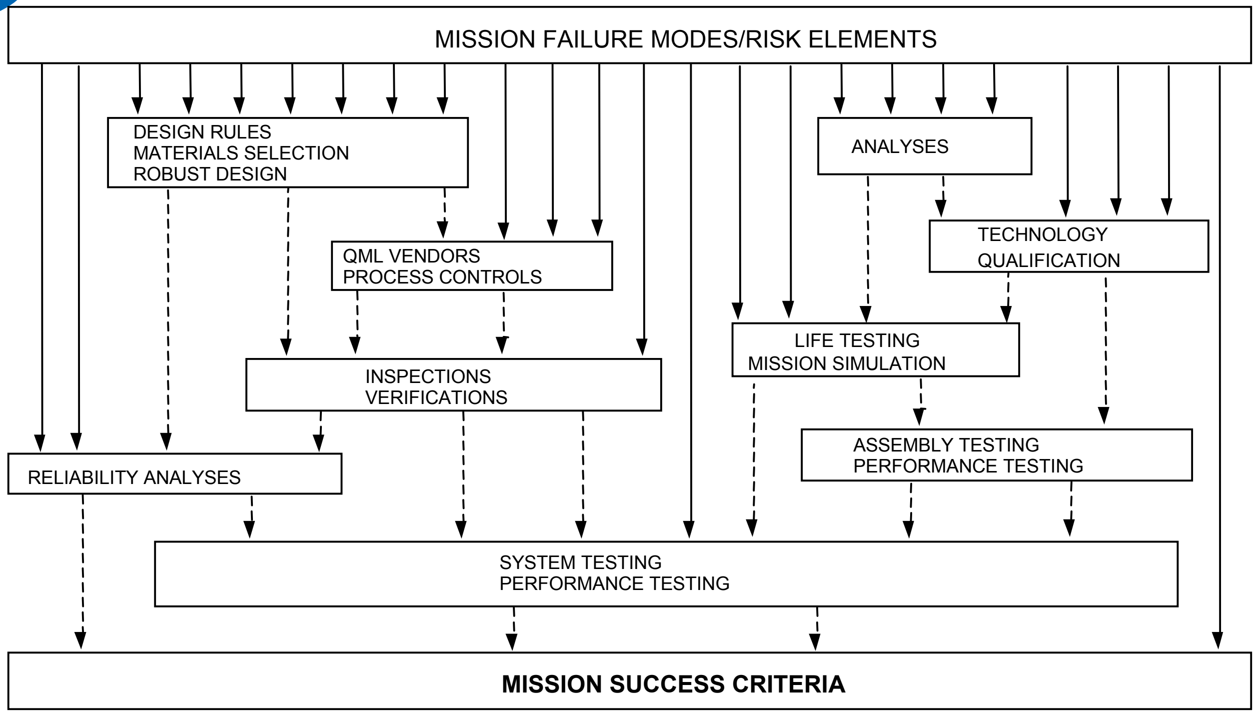
<u>Approach</u>

- Code Q has funded the development of "tools which address residual risk as a function of various risk control options. Options exist at the planned activity level and in the degree to which potential failure modes are addressed."
  - DDP tool has module containing data from ongoing Code Q Failure Detection and Prevention Program (joint GRC/GSFC/JPL RTOP)
  - DDP Version 2.0 VB has been released, Version 2.5 VB/1.5 Java due in early summer
- Have formed partnerships/pilot studies with technologists and mission designers within NASA and JPL, other teaming outside NASA being explored.

AGENDA

- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

“Screening Out” the Defects



Notes:
1) Each box is a collection of PACTs
2) Dotted lines represent “escapes” - Undetected or un-prevented failure modes
3) Illustrative diagram only - nothing is “to scale”

PACTs - Are everything that could be done (e.g. “toolbox” of prevention/detection options)

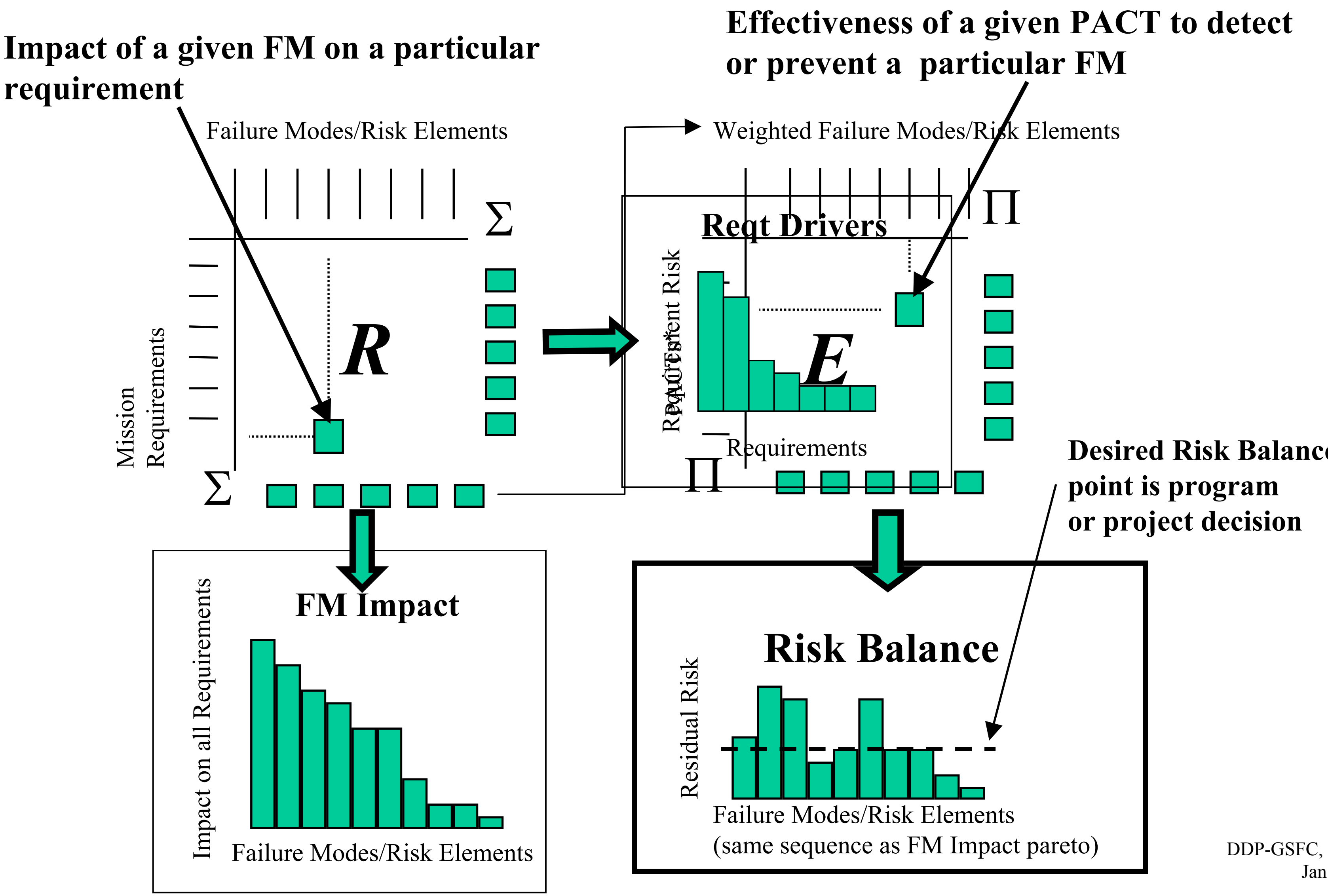
- **P**reventative measures (Redundancy, Design Rules, Materials Selection, Software Architecture, etc.)
- **A**nalyses (Reliability (Fault Tree Analyses, Failure Mode and Effects Criticality Analysis (FMECA), Worst Case Analysis), Fatigue, Structural, Performance, Electrical SPICE models, etc.)
- process **C**ontrols (Inspections, Materials purity, QML vendors, Documentation, etc.)
- **T**ests (Environmental, Life, Simulations, Performance, etc.)

Failure Modes (**FM**s)/Defects/Risk Elements

- Failure is used in its broadest sense: Failure to meet goals/requirements
- “Hard” - Cracks, Explosions, Open Circuits, etc.; “Soft” - Resets, Performance Degradations, etc.

Simplified DDP Summary

•DDP utilizes two matrices: the Requirements matrix (***R***) and the Effectiveness matrix (***E***)



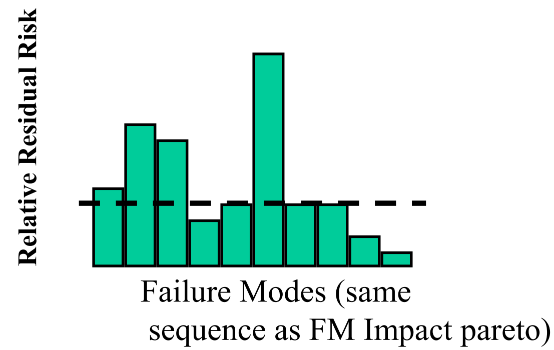
Overview of the DDP process

- What does the DDP process/tool do?
  - Allows users to perform a variety of risk management activities
- What inputs does the DDP process/tool require?
  - Information can be pre-existing
    - FDPP PACT Effectiveness ‘pre-canned’ information or previous DDP evaluations
    - Existing schedules, preliminary risk elements and mitigation options
    - Requirements trees, fault trees, etc. at various levels of importability
  - Information can be entered prior to sessions or in ‘real time’
    - Project Requirements and their relative weights
    - Article Trees (breakdown of system into subsystems into assemblies, etc.)
    - Failure Modes and Risk Elements (from high-level categories to low-level mechanisms)
    - PACT options (from high-level types to specific activities)
- What are the outputs of the DDP process/tool?
  - **Identify areas requiring additional work or more detailed analysis**
  - **Driving requirements** (requirements which are producing the most risk)
  - **Risk Balance** (Can sort by risk type, articles affected, etc.)
    - Under-covered risk elements (‘tall poles’)
    - Over-covered risk elements (move the resources elsewhere)
  - **PACT selection** (Can sort by risk type addressed, articles requiring PACTs, etc.)
    - PACTs agreed upon to achieve desired risk balance (incl. Costs)
    - Value of remaining un-selected PACTs

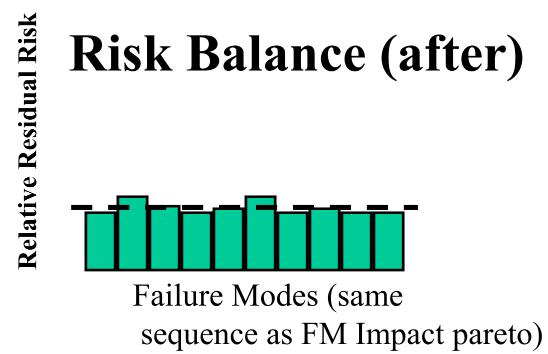
Using DDP to Tailor and Optimize

- Risk Balance
  - The residual risk is the 'expected value' of the failure mode, i.e, the product of it's likelihood, severity and chance of escaping
  - Measures product of how much we care and chance we will miss it
- Risk balancing trades off PACT options against residual risks
  - Versus constraints (mass, power, $, etc.)
  - Can shift priorities
  - Select different PACT combinations
  - Capture design and PACT decisions
  - Modified/refined with project life cycle

Risk Balance (before)



Risk Balance (after)



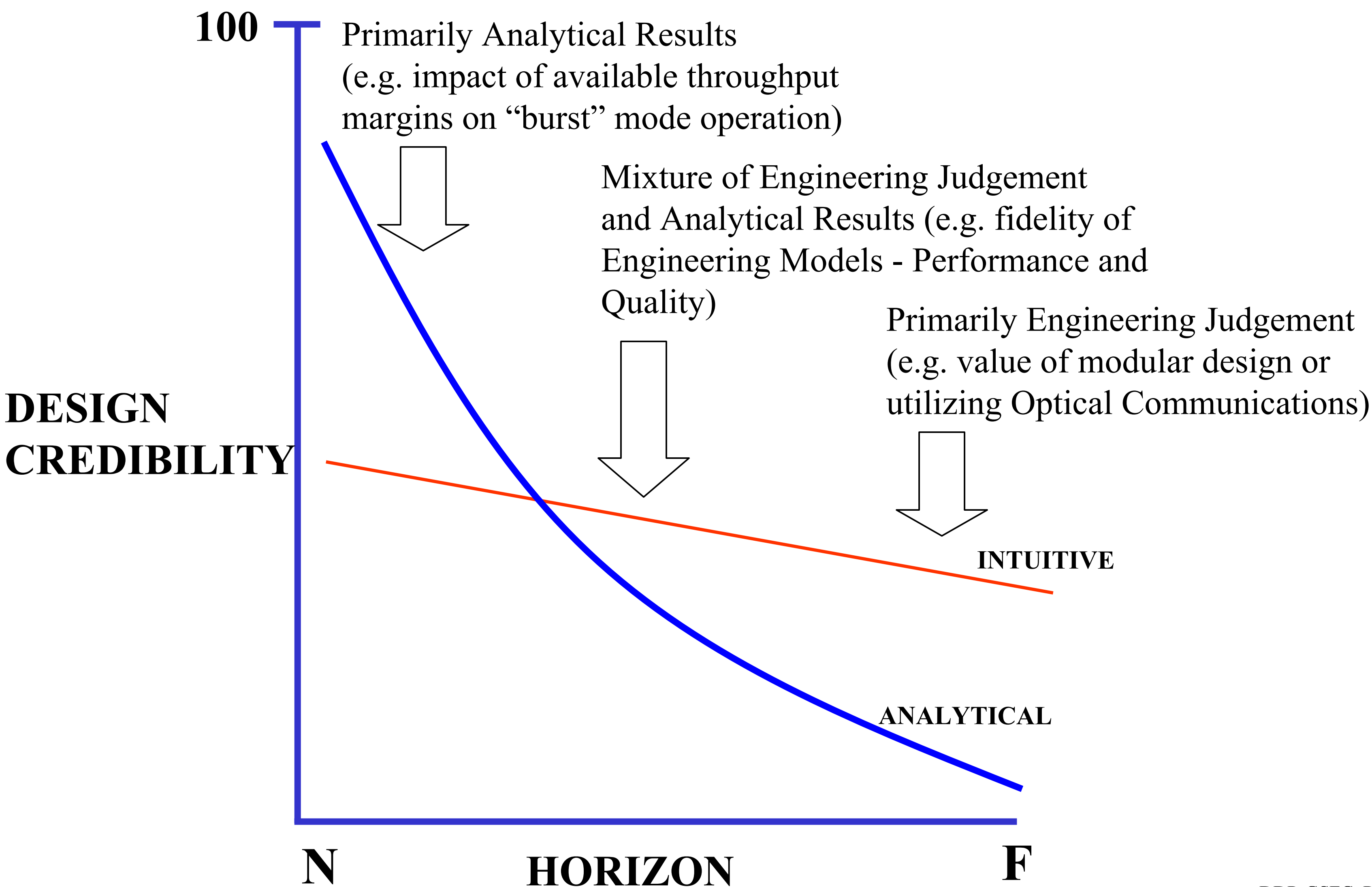
For each failure mode:

Residual Risk = r = i x e =The extent of it's impact x How likely it will occur

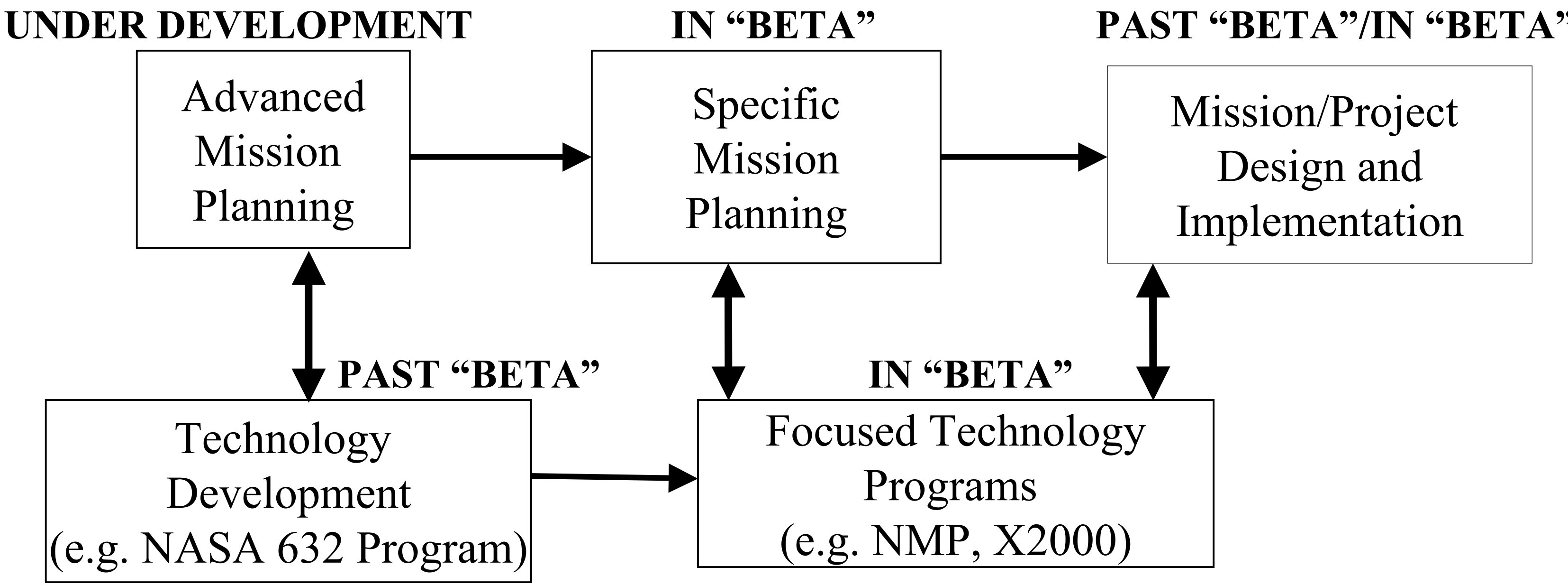
AGENDA

- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

DDP integrates intuitive and analytical approaches



DDP usage in the NASA Mission timeline



- The concept of "What are we trying to accomplish, what could get in our way and what can we do about it" is very broad
  - Level of fidelity grows with project/program design maturity
  - Can be applied in a number of places in the NASA Mission timeline
  - Have done a wide variety of "alpha", "beta" and more, pilot applications
  - Real power is in getting the right team together and quickly, systematically integrating quantitative and qualitative information

Applications of DDP to date

	Technology Portfolio/Options	Project Risk Management
Mission Suites	Pending	
Mission	Pending	ConX?, MER?, Mars05?, Europa Orbiter?, StarLight Instrument?, Others?
System/subsystem	XYZ	TIMA, DS1, DS2, ST3, XYZ
Assembly	various examples	TIMA, DS2, X2000, ST3, NCMS
Device/Component	various examples	TIMA, NCMS, DS2, ST3, MGS, RelTech
PACT Suite	various examples	FDPP, DfS?
Individual PACT Tailoring	various examples	FDPP, many examples

ST3= Space Technology 3
TIMA=Technology Infusion and Maturity Assessments
DS1= Deep Space 1
DS2= Deep Space 2
X2000= Electronics Packaging portion of the X2000 project

NCMS=National Center for Manufacturing Sciences collaboration
RelTech=Collaboration to insert Advanced Packaging
MGS=Mars Global Surveyor extended mission
FDPP=Code Q's Failure Detection and Prevention Program
DfS=NASA's Design for Safety Program
XYZ=Recent JPL Project assessment

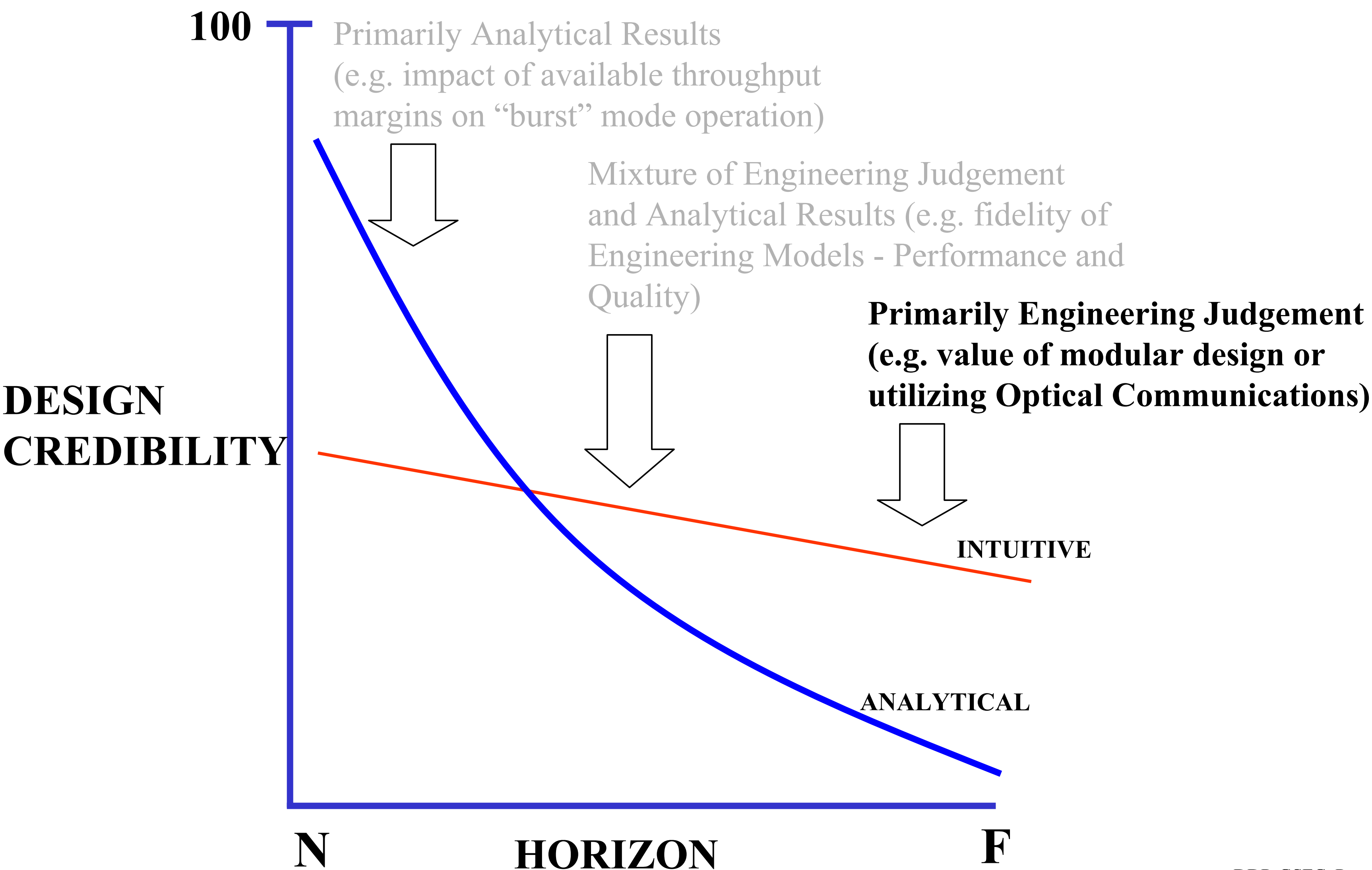
AGENDA

- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- $\boxed{\text{TOOL DEMONSTRATION}}$
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

AGENDA

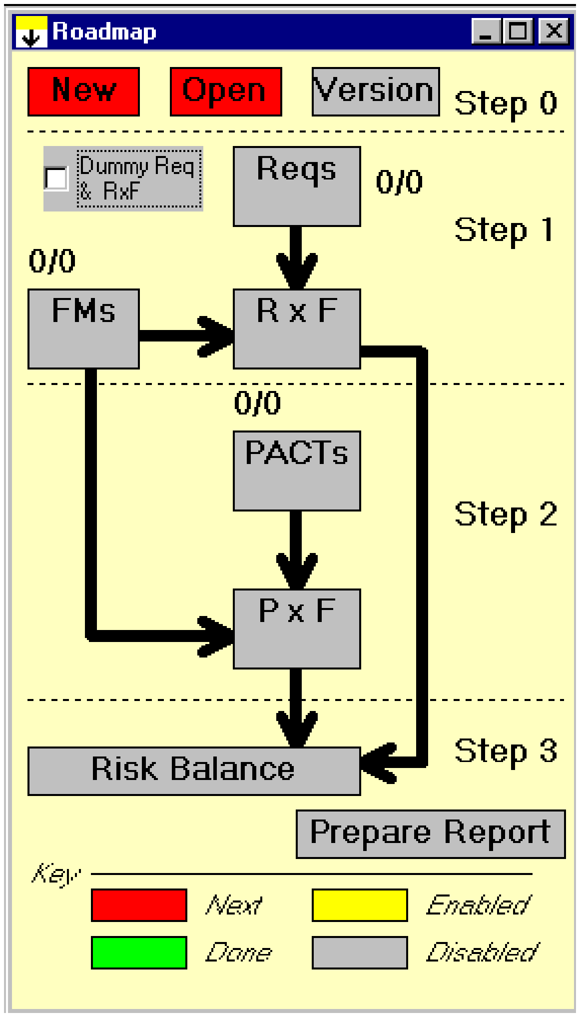
- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

DDP integrates intuitive and analytical approaches Application to Advanced Technology “Roadmapping”



Roadmap for DDP sessions

•Perform over 4 (or 3) half-days



Day1: Understand the Technology - lots of questions, no judgement on adequacy, etc.

Day2: Develop the Requirements matrix. Identify top-level (and lower-level) requirements, possible failure modes (if nothing is done to prevent/detect) and score impact should the failure modes occur

Day3: Develop the Effectiveness matrix. Identify top-level (and lower-level) PACTs, use already identified failure modes and score effectiveness of PACTs at detecting/preventing the occurrence of the failure modes.

Day4: Select the combination of PACTs which minimize the risks [subject to various constraints (time, $, etc.)]

DDP applied to technologies

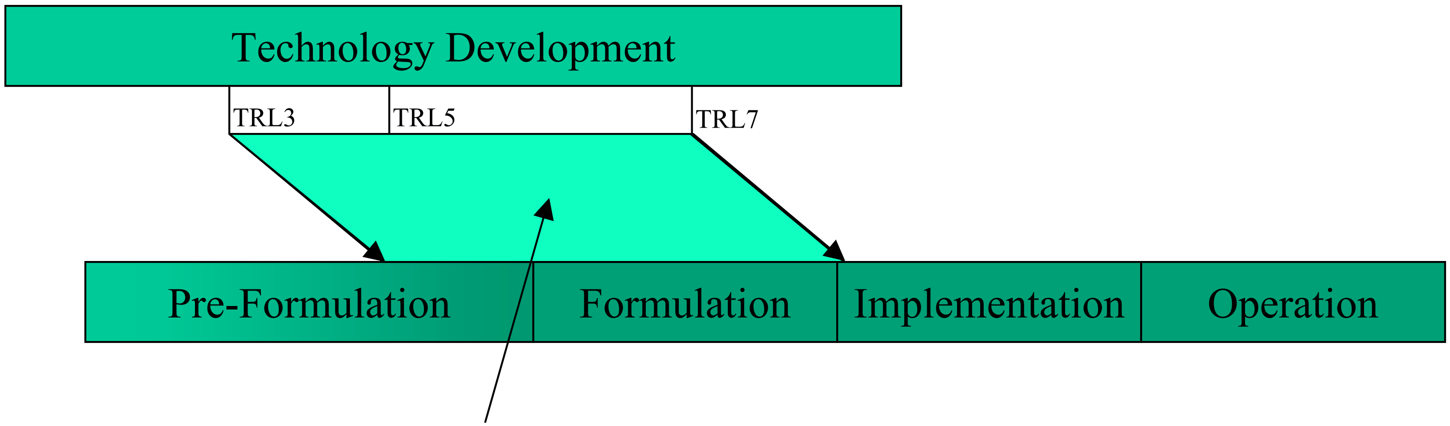
(Technology Infusion and Maturity Assessment (TIMA))

- Hybrid Imaging Technology (HIT) - Cost: 10k$
  - Saved $600k radiation fabrication effort and $300k ground test program
  - HIT product delivery to customer in ‘00 versus ‘02-’03
  - Task alignment with flight implementation expertise
- Compact Holographic Data Storage (CHDS) - Cost: 12k$
  - Focused on SNR and BER issues (major show stoppers) **not** memory volume
  - Increased focus on breadboard development (migrate technology off the optical bench)
  - Identified required analysis and proof tests
  - Alignment with other ongoing R&D (NEPP) and Sandia
- Variety of Others
  - National Instruments’ LabView software - Cost: about 10k$
  - Active Pixel Sensor (APS) program - Cost: about 10k$
  - Micro-gyro program - Cost: 9k$
  - ITP/SIM - Cost: varied
  - Commercial Industry (disk drives, avionics)

Successes on technology evaluations

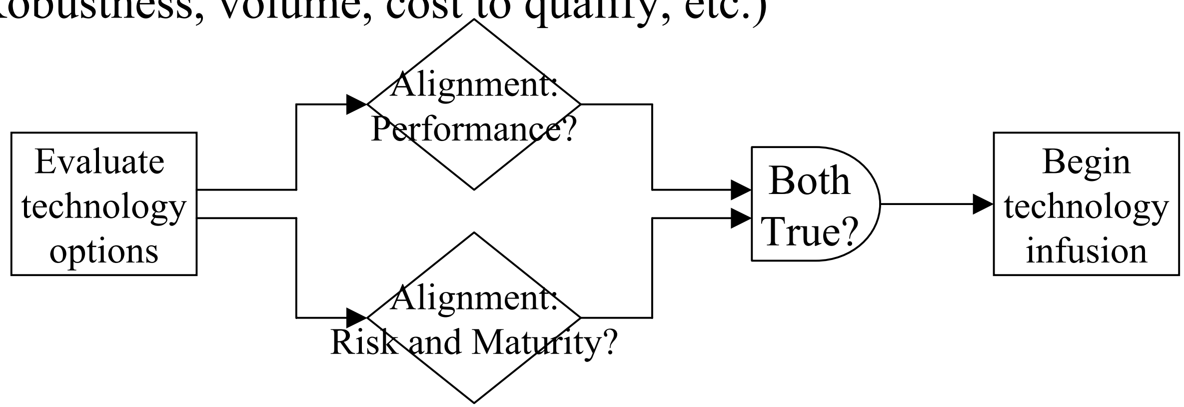
- Have resulted in an "institutionalization" of the process at JPL within the technology community
  - Will continue applying to "Proof-of-concept" and earlier technologies
  - Will begin to quantitatively validate the process in the lab
  - Will begin applying to more far-horizon mission studies
  - I have a joint appointment between the Safety and Mission Assurance and Technology Applications Directorates at JPL to help make this happen

Technology Infusion Process (JPL process in draft)



This portion should NOT be a discrete hand-off

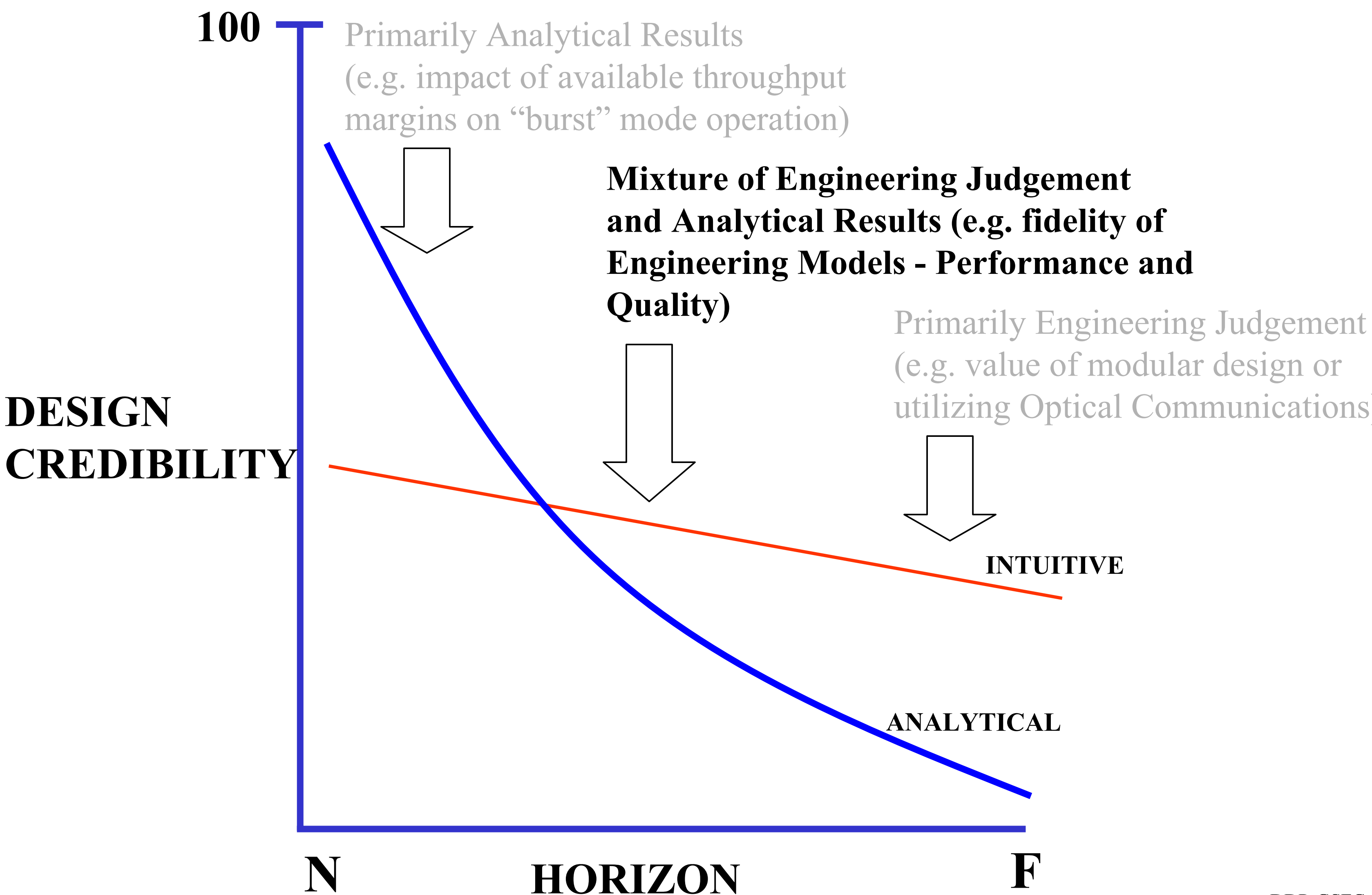
- It should be more like a phase-locked loop
- Developmental milestones/roadmap agreed upon
- Look for more than just nominal performance
  (Robustness, volume, cost to qualify, etc.)



AGENDA

- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

DDP integrates intuitive and analytical approaches
Application to Mission and System Design



Information and Influence by Project Phase (Formulation)

Project Phase	Available Information	Questions to be answered	FDPP Applicable Products
Formulation	•Science Goals •Project Teaming •Subsystem Types and Requirements •Launch Vehicle •Preliminary Trajectory •Technology Requirements •Risk Posture •Schedule •Etc.	**•Architectural Options** **•Mission Design Options** **•System Design Options** •Heritage Applicability •Environmental Concerns •Verification and Validation Approaches •Redundancy and SPF Policies **•Schedule and Cost feasibility** **•Risk Management Policy** •Margin Philosophy •Etc.	•FDPP Guidebook -Introduction -Risk as a Resource -Anomaly Trends •RBP Tool •DDP Tool (higher level evaluations)
Implementation: Prelim Design	•Medium-level Information	•Medium-level questions/answers	•FDPP Guidebook •DDP Tool
Implementation: Detailed Design/ATLO	•Detailed-level Information	•Detailed-level Information	•FDPP Guidebook •DDP Tool

SUMMARY OF RECENT APPLICATION TO ARCHITECTURAL ASSESSMENT

- Primary Areas of Assessment
  - **Sensors
  - **Heat Rejection
  - *Avionics Architecture
  - **Signal Processing
  - *Processor
  - *Upset Immunity
  - *Thermal Control
  - **FPGAs
  - Structure
  - **Operational Modes
  - *Materials and Parts
  - Software

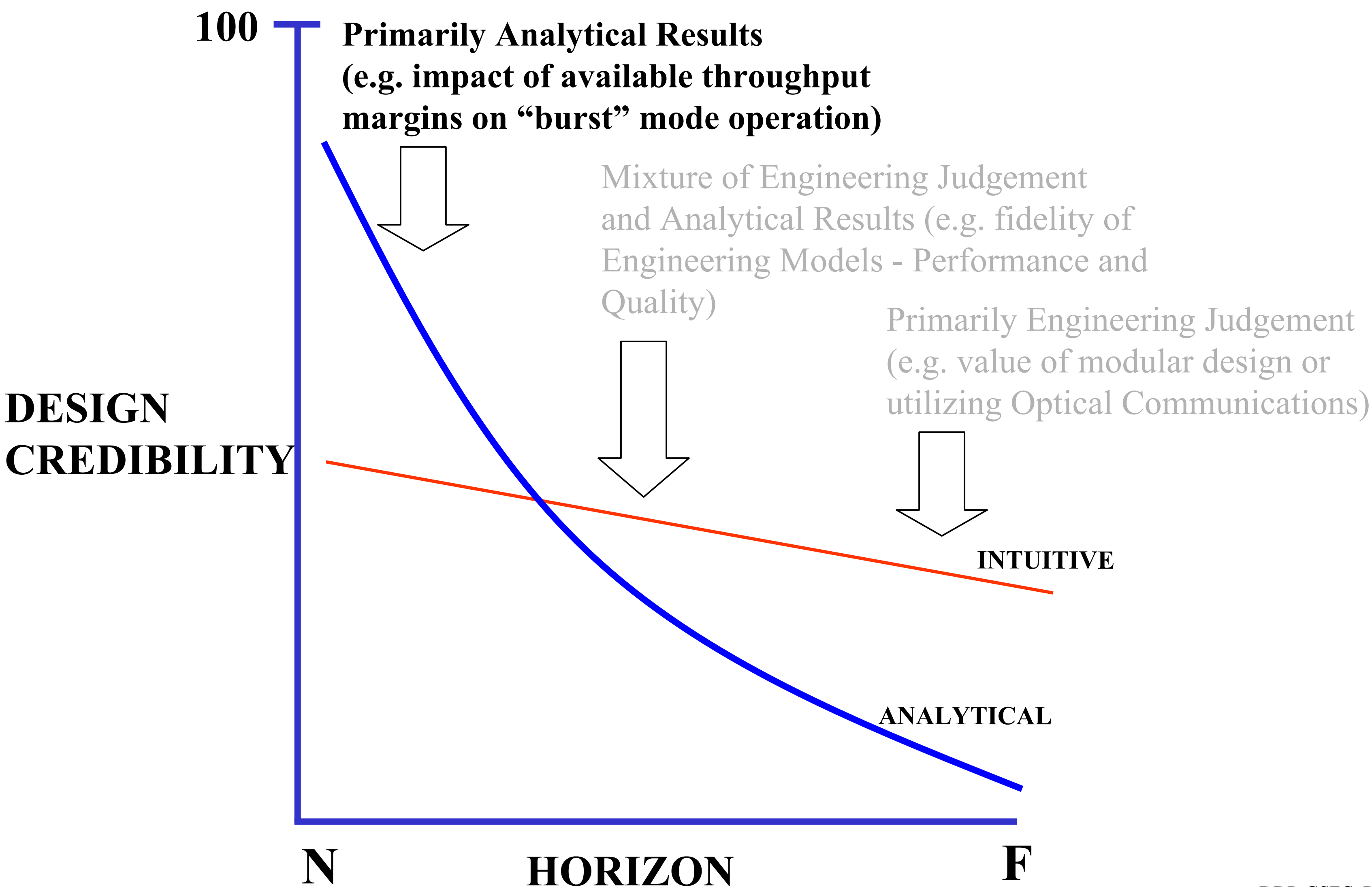
** = Significant pay-off
* = Moderate pay-off

- Results of three 1/2 day sessions (Total cost: <14k$):
  - Savings of at least 2.5 M$, 154 W (and reduced radiators), and 22 kg.
  - Project action items:
    - Ripple effects not entirely included (will make it better)
    - Some decisions require further analysis (potential savings of 5-8M$, etc.)

AGENDA

- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

DDP integrates intuitive and analytical approaches
Application to Project Implementation



Information and Influence by Project Phase (Preliminary Design)

Project Phase	Available Information	Questions to be answered	FDPP Applicable Products
Formulation	•High-level information	•High-level questions/answers	•FDPP Guidebook •RBP Tool •DDP Tool
Implementation: Prelim Design	•Unit-level requirements •Environmental exposures and estimates •Functional Block Diagrams •Engineering Resource Allocations •Parts/Material/Process Candidates •Heritage Reviews •Etc.	•Long-lead item requirements •Environmental Levels •Reliability Estimates •Verification and Validation Plans •Part-type/material/process selection •Mission Assurance Support Distribution •Developmental and Engineering Model scope •Detailed cost profiles/reserves •Detailed schedules/reserves •Current risk landscape •Margin approach •Etc.	•FDPP Guidebook - Failure Mode Types -PACT Effectiveness Evaluations -PACT Tailoring •DDP Tool (medium level evaluations)
Implementation: Detailed Design/ATLO	•Low-level information	•Low-level questions/answers	•FDPP Guidebook •DDP Tool (lower level evaluations)

Information and Influence by Project Phase (Detailed Design/ATLO)

Project Phase	Available Information	Questions to be answered	FDPP Applicable Products
Formulation	•High-level information	•High-level questions/answers	•FDPP Guidebook •RBP Tool •DDP Tool
Implementation: Prelim Design	•Medium-level information	•Medium-level questions/answers	•FDPP Guidebook •DDP Tool (medium level evaluations)
Implementation: Detailed Design/ATLO	•Detailed Functional Requirements •Circuit Diagrams and Detailed Drawings •Part/Material/Process selections •Layouts and CAD models •Analyses and Evaluation Results •Developmental Test Results •Etc.	•Test Levels and other details •Analysis Applicability •Acceptance criteria •Rework/retest decisions •Anomaly resolution and close-out •Specific risk evaluations •Inspections •Management processes •Margin status/reserve •Other project implementation details	•FDPP Guidebook - Failure Mechanism Information -PACT Effectiveness Evaluations -PACT Tailoring •DDP Tool (lower level evaluations)

DDP Implementation in the Project Implementation phase

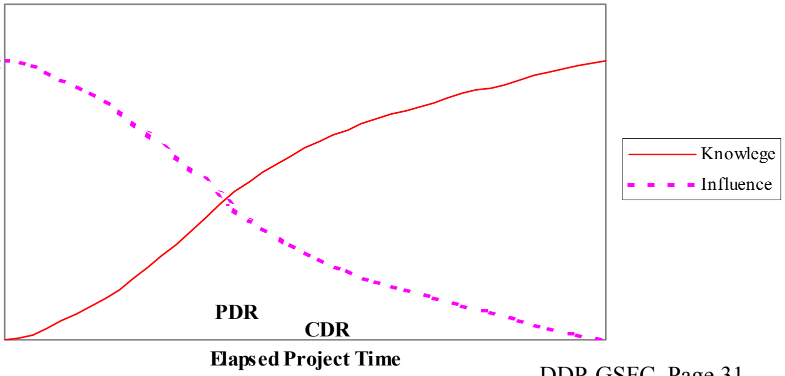
- Have performed at all levels of assembly
  - System, sub-system, assembly, sub-assembly, device, die
- Have performed on a variety of subsets
  - Specific “root causes” (FMECA-type)
  - Various risk element types (FTA-type)
  - Specific exposure environments
- Have FY01-03 budget to begin piloting several “cradle-to-grave” implementations on NASA flight projects
  - IPAO is beta-testing DDP in upcoming assessment of JPL flight project
  - A number of project options exist
    - Various characteristics
    - Various design maturity levels

AGENDA

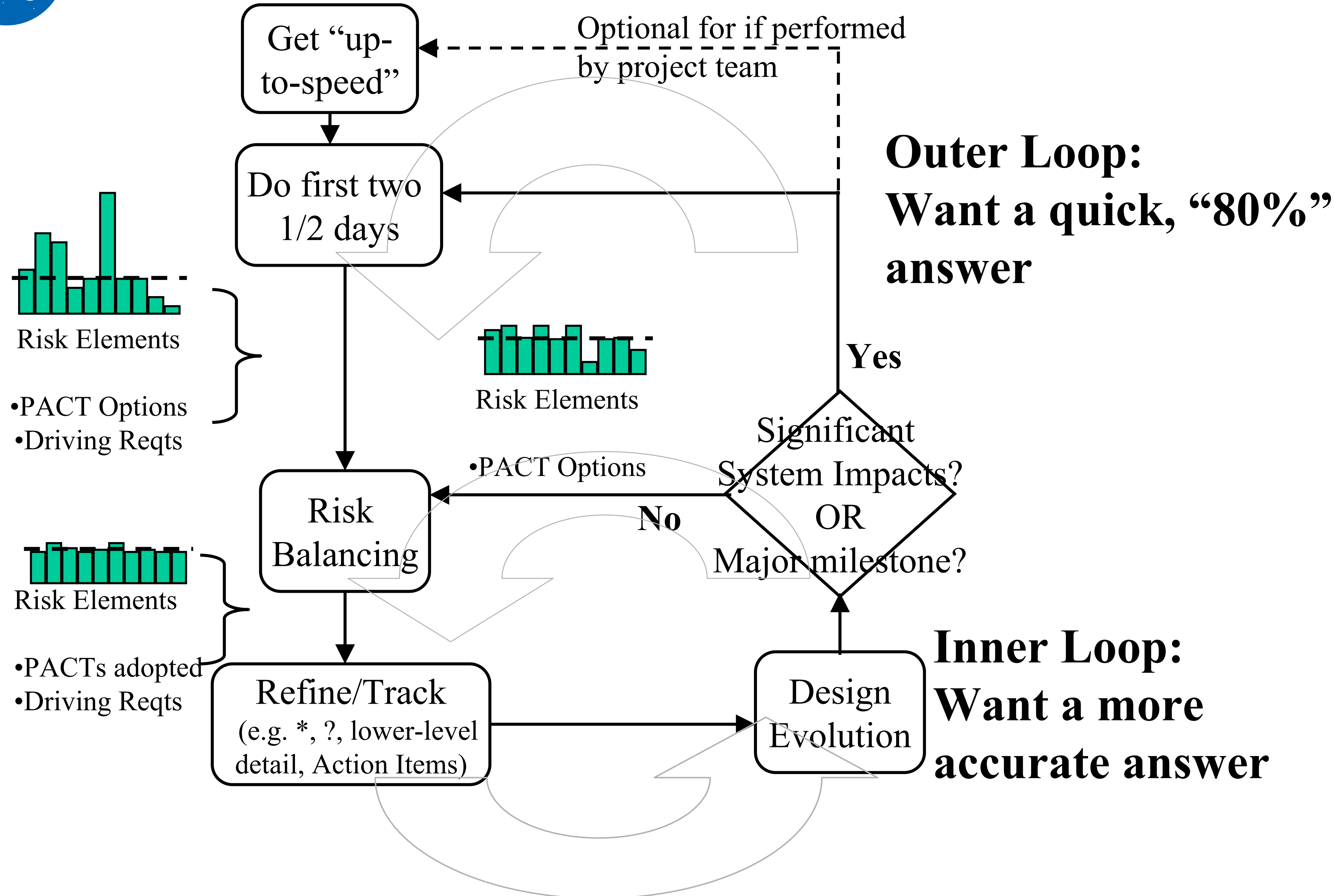
- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

DDP Process Implementation

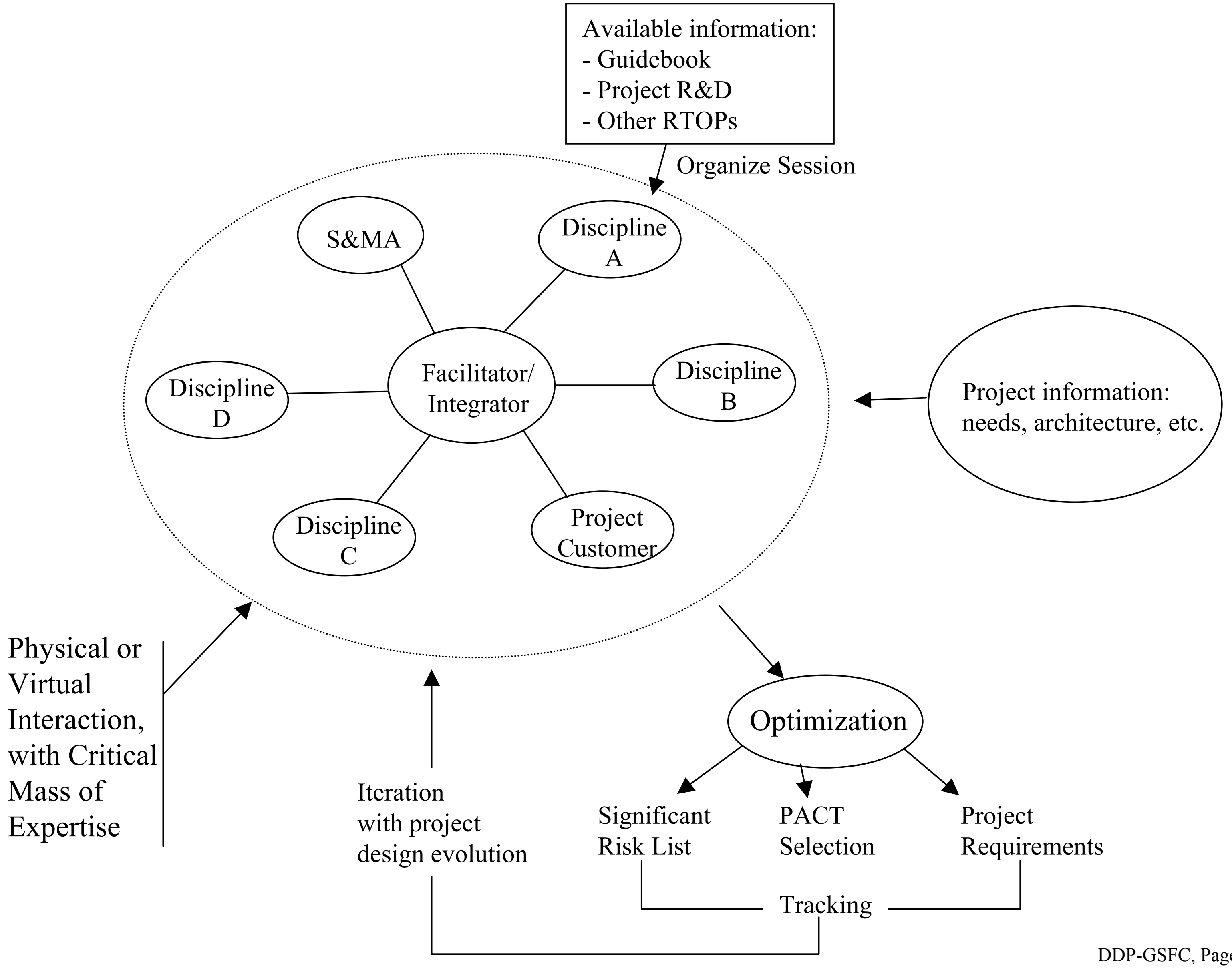
- Initial brainstorming
  - Understand the technology, architecture, mission, etc.
  - Requires ‘critical mass’ of relevant expertise
  - Use tool in ‘Design Center mode’ - real or virtual
  - Use disagreements to guide the depth of evaluation
    - Go into detail required to ensure adequacy of the evaluation
    - Take from religious discussions into engineering discussions
- Converge on baseline
  - Identify areas which could still benefit from additional information
  - Evaluate resource costs of baseline PACTs and select baseline
  - Identify ‘tall pole’ residual risks (Significant Risk Lists)
- Iterate with project life cycle
  - The fidelity evolves with the project life cycle
  - Incorporate changes as they occur
  - Make real-time adjustments in PACT implementation



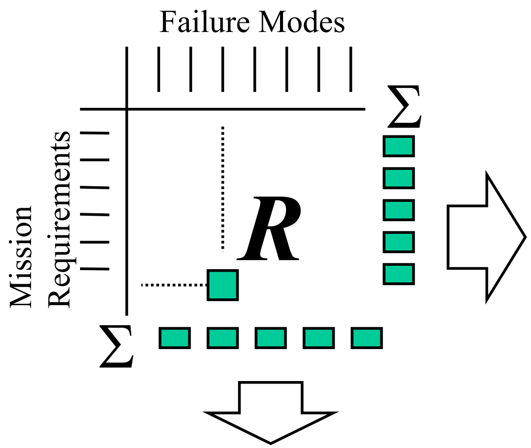
Flow chart for DDP implementation



DDP Process Summary

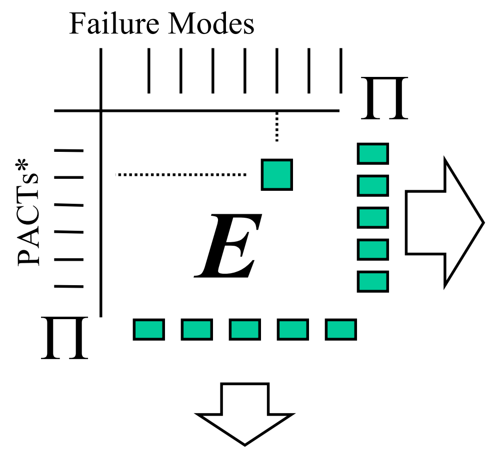


Detailed DDP Summary



Sum on each Row yields ***d***, the extent to which each mission requirement is impacted by the FMs

Each column sum yields ***i***, the extent to which each FM impacts success



Product of elements within a Row yields ***f***, figure of merit for each PACT*

Product of elements within each Column yields ***e***, the PACT* coverage for each failure mode ("Escape" chance)

Note: Including requirement criticalities, ***C***, and FM likelihood, ***L***, yields weighted Requirements Matrix: ***R'***=[***C***]***R***[***L***]

For each failure mode:

Residual Risk = r = i x e =Extent of it's impact x Probability it will still occur

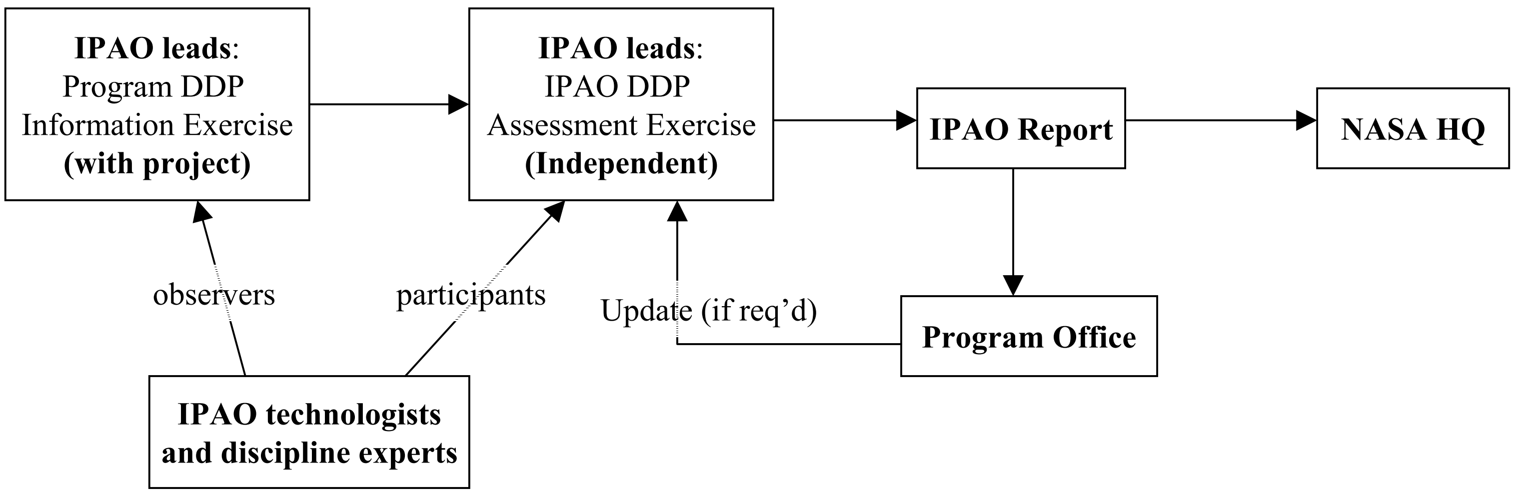
* PACTs=**P**reventative measures, **A**nalyses, process **C**ontrols and **T**ests

Note: $\prod$ is the product symbol (a1*a2*…), $\sum$ is the summation symbol (a1+a2+…)

AGENDA

- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

Proposed process for DDP implementation by IPAO



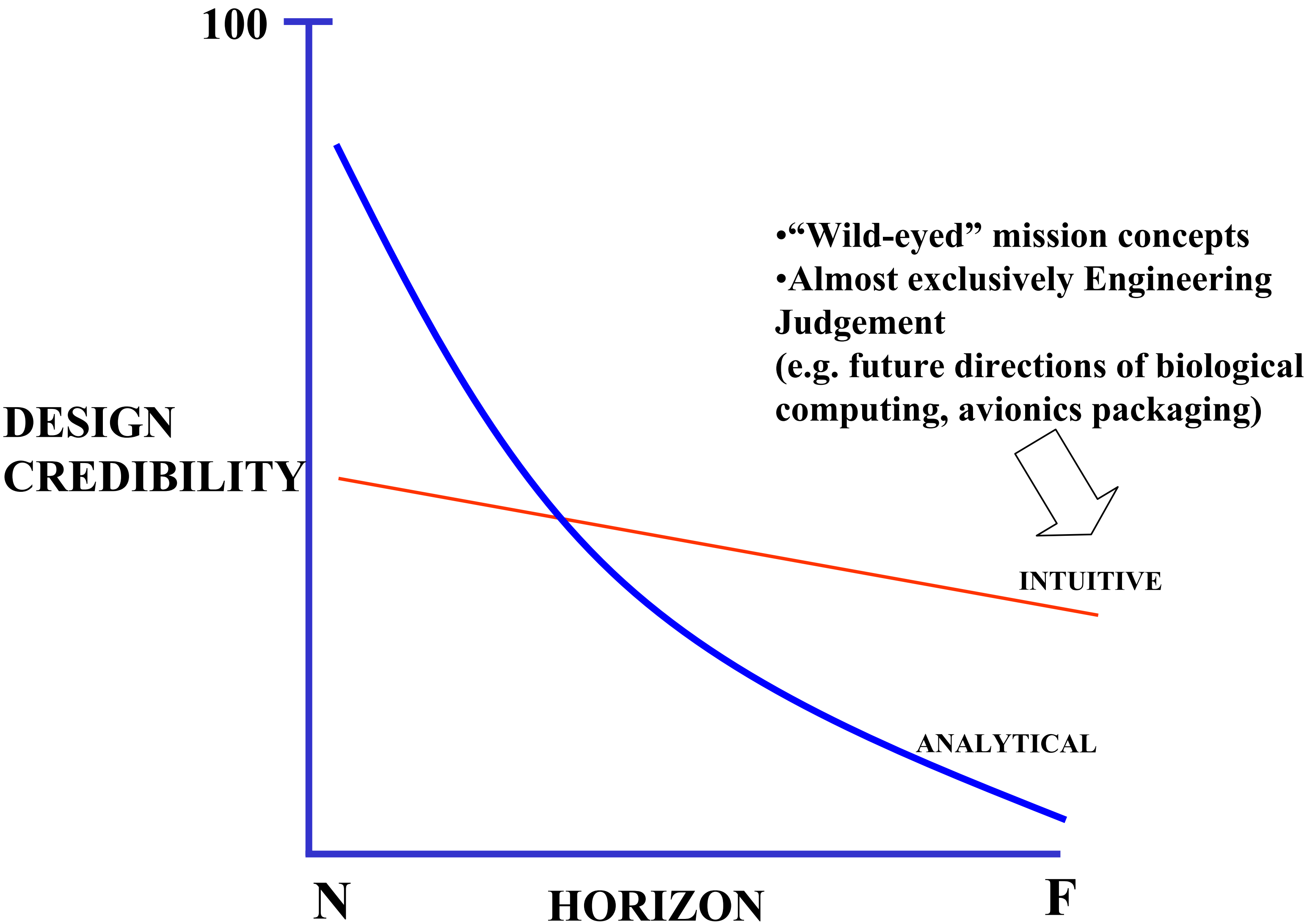
- Could help IPAO personnel incorporate risk into their assessments
- Could help IPAO assessments remain independent but operate from a position of 'being up to speed'
- We are trying this out on a JPL project in the near future

Notes: If project already using DDP, box at upper left may just be a walk-through of their existing information

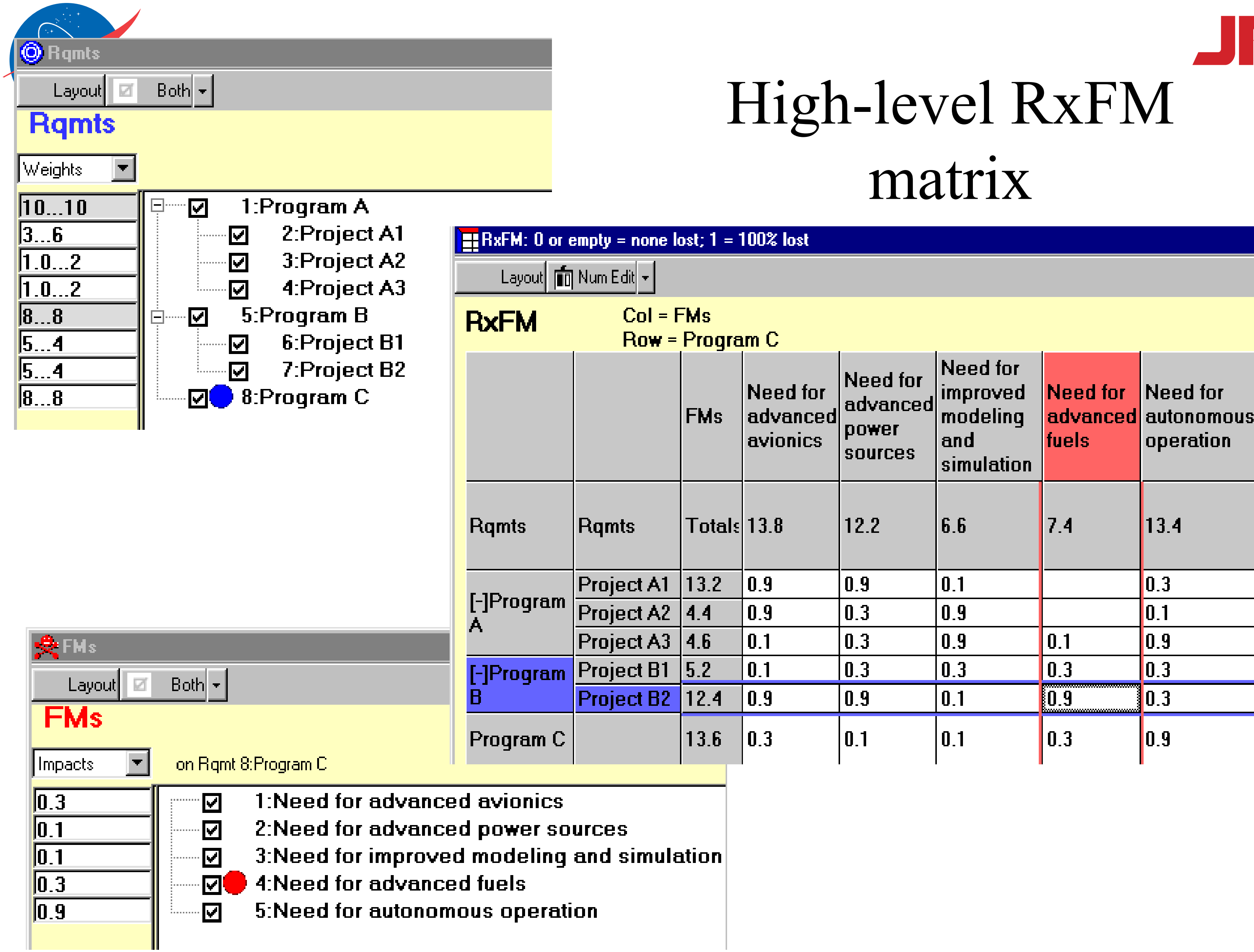
AGENDA

- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

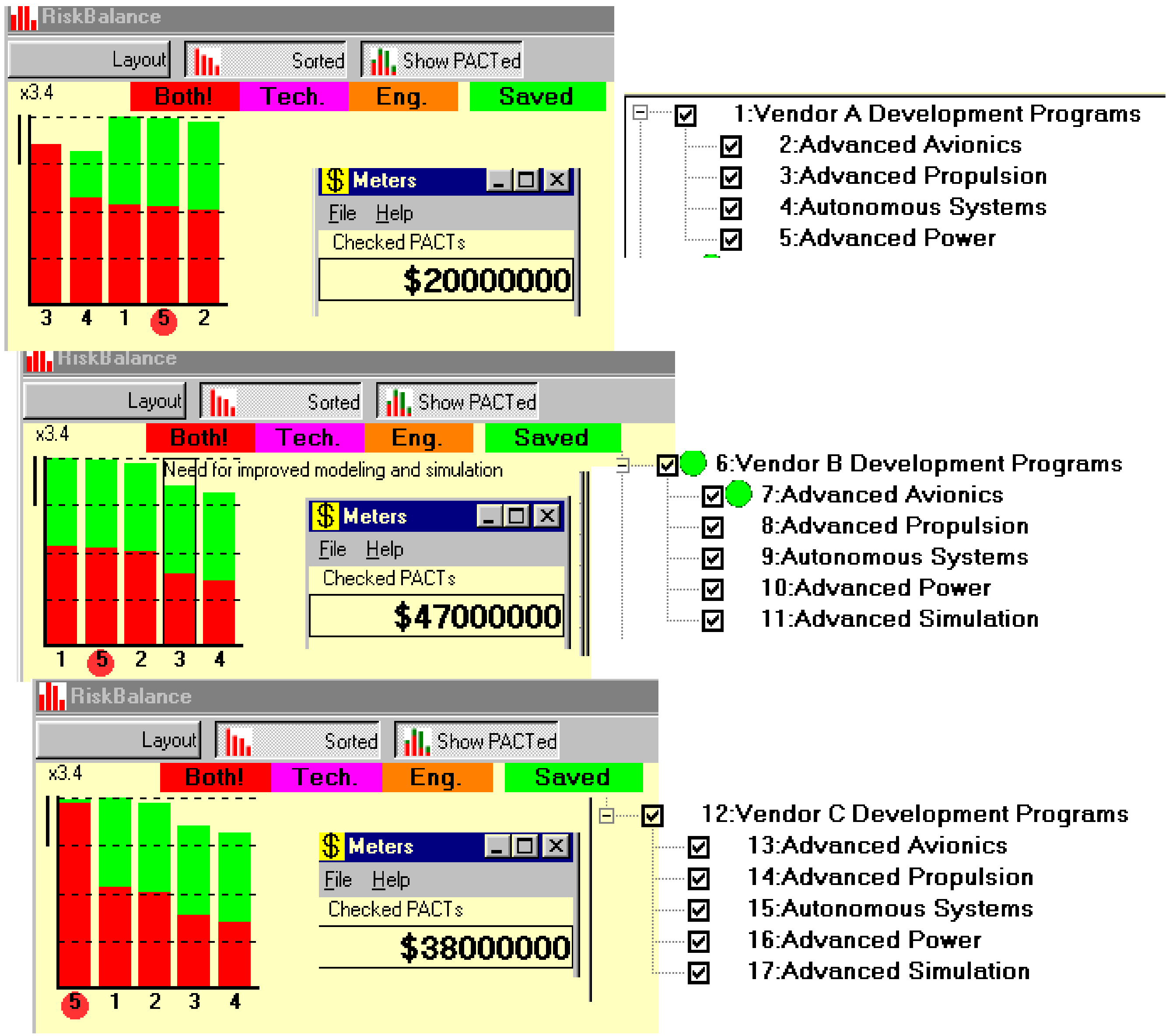
DDP integrates intuitive and analytical approaches Application to Technology Portfolio Development



High-level RxFM matrix

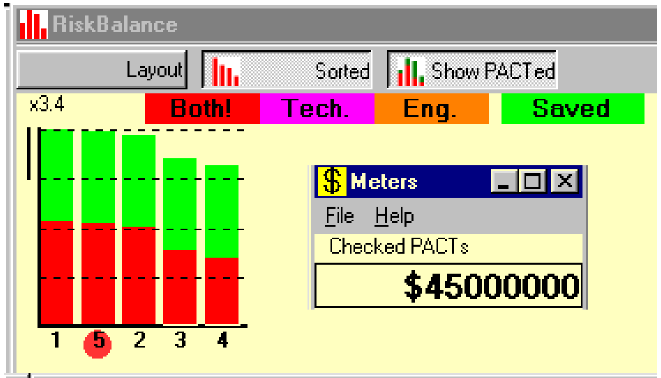


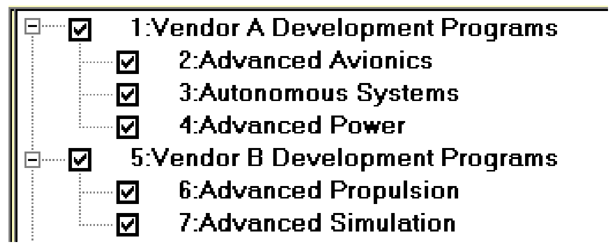
High-level investment decision

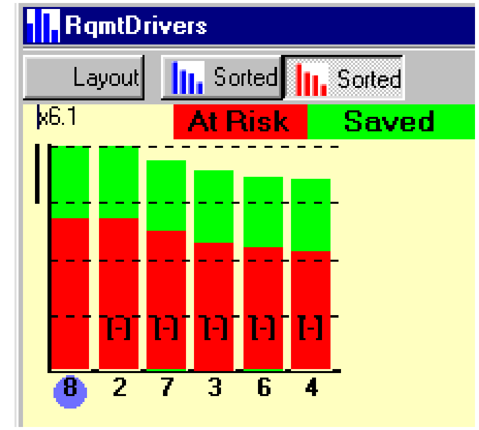


Optimizing the high-level decision

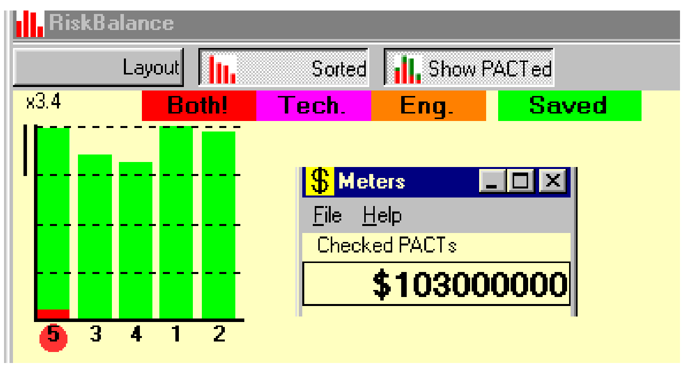
No overlap

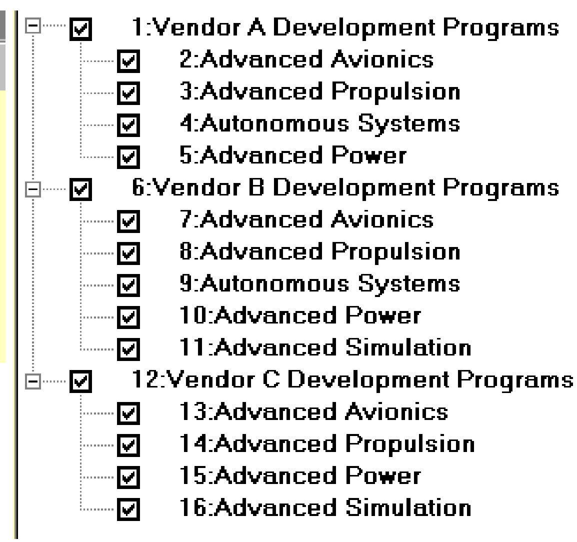


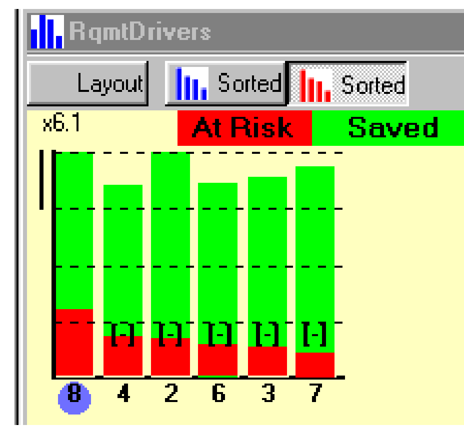




Minimal Risk







Refined RxFM matrix

1:Need for advanced avionics
- 2:MIPS
  - 3:MIPS = 1k
  - 4:MIPS = 10k
- 5:Memory
  - 6:Volatile
    - 7:Volatile = 1 TByte
    - 8:Volatile = 10 TByte
- 9:Mass
  - 10:Mass < 2.0 kg
  - 11:Mass < 0.5 kg

12:Need for advanced power sources
13:Need for improved modeling and simul
14:Need for advanced fuels
15:Need for autonomous operation

RxFM: 0 or empty = none lost; 1 = 100% lost

Layout | Num Edit

RxFM Col = Volatile = 10 TByte
Row = Project A1

Rqmts

Layout | Both

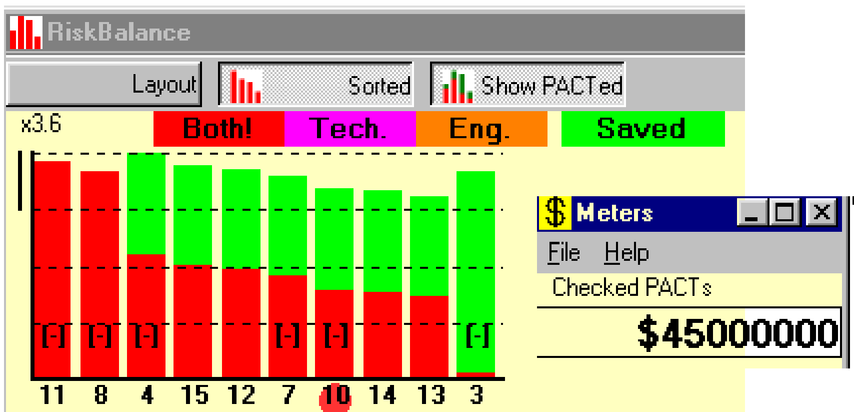
Rqmts

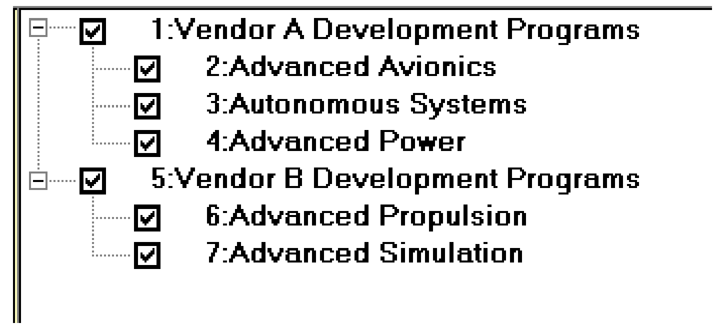
Weights

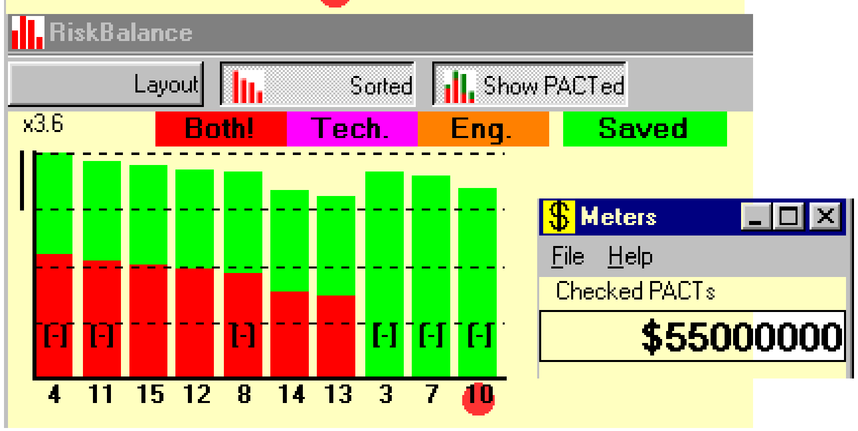
Weights	Rqmts
10...10	1:Program A
3...6	2:Project A1
1.0...2	3:Project A2
1.0...2	4:Project A3
8...8	5:Program B
5...4	6:Project B1
5...4	7:Project B2
8...8	8:Program C

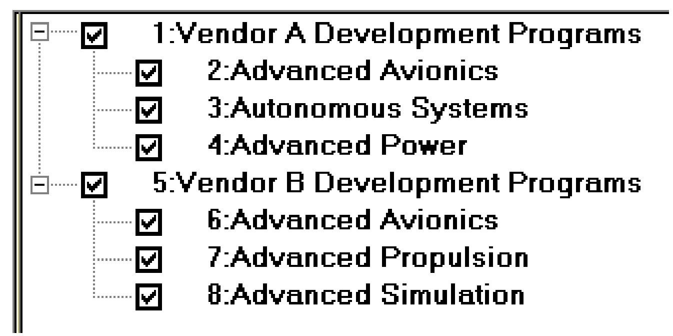
		FMs	[-]Need for advanced avionics						Need for advanced power sources	Need for improved modeling and simulation	Need for advance fuels	Need for autonomous operation
		FMs	[-]MIPS		[-]Memory		[-]Mass					
		FMs	MIPS = 1k	MIPS = 10k	[-]Volatile		Mass < 2.0 kg	Mass < 0.5 kg				
		FMs			Volatil = 1 TByte	Volatil = 10 TByte						
Rqmts	Rqmts	Totals	11.6	17.5	10.6	11.52	7.8	14.7	12.2	6.6	7.4	13.4
[-]Program A	Project A1	41.82	0.9	0.99	0.9	0.99	0.9	0.99	0.9	0.1		0.3
	Project A2	10.38	0.1	0.9	0.9	0.99	0.1	0.9	0.3	0.9		0.1
	Project A3	7.2		0.1	0.1		0.3	0.9	0.3	0.9	0.1	0.9
[-]Program B	Project B1	6			0.1		0.1	0.1	0.3	0.3	0.3	0.3
	Project B2	22.32	0.9	0.99	0.1	0.3	0.1	0.99	0.9	0.1	0.9	0.3
Program C		25.6	0.3	0.7	0.3	0.3	0.1	0.1	0.1	0.1	0.3	0.9

Deeper penetration provides additional insight









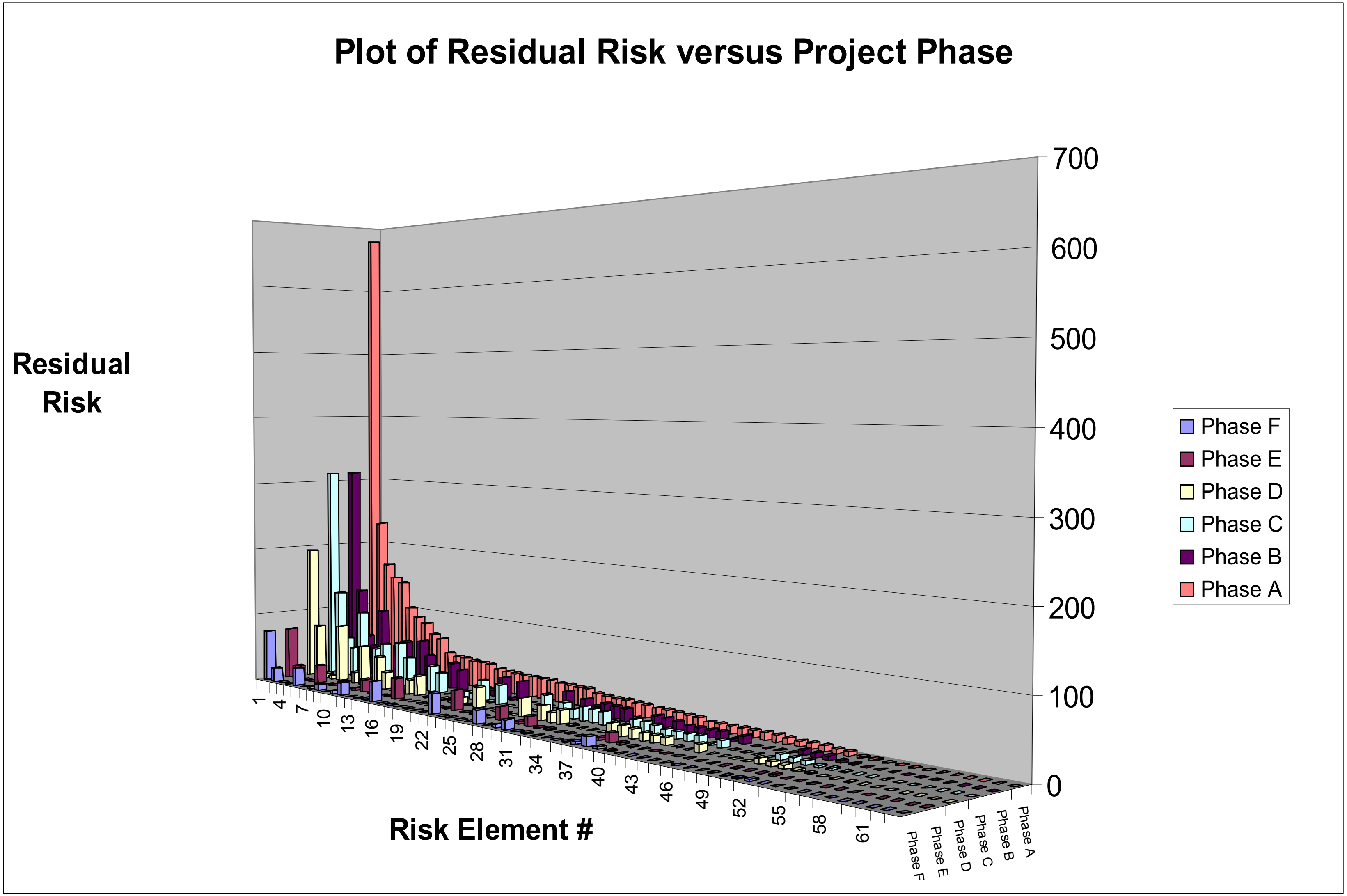
AGENDA

- BACKGROUND
- INTRODUCTION TO THE DDP PROCESS
- APPLICABILITY OF THE DDP PROCESS
- TOOL DEMONSTRATION
- APPLICATION TO:
  - ADVANCED TECHNOLOGY ROADMAPPING
  - MISSION AND SYSTEM DESIGN
  - PROJECT IMPLEMENTATION/OPERATION
- IMPLEMENTING THE DDP PROCESS
- APPLICATION TO:
  - INDEPENDENT PROGRAM ASSESSMENTS
  - TECHNOLOGY TRADES/PORTFOLIOS
- SUMMARY AND CONCLUSIONS

Using DDP to do Risk Management

- Risk Identification
  - Initial Brainstorming
  - Complete Evaluation
- Risk Analysis
  - Initial Brainstorming
  - Tall Pole Risks
  - Driving Requirements
- Risk Planning
  - PACT Options and PACT Adoption/Selection
  - What-if scenarios
  - Generate Baseline
- Risk Tracking
  - Assess adequacy and implementation status of planned PACTs, Identify new risk elements
- Risk Control
  - Refine Requirements, PACTs, and Risk Elements with project/program evolution

Navigating the risk landscape



Summary

- The DDP process has been described:
  - A process for achieving clear and continuous insight into the evolving risk landscape
  - Level of detail as required for application and project life cycle
    - Usage ranges from mission theme planning, to project planning and implementation to detailed technology evaluations
    - Fidelity grows with design maturity
    - Provides a vehicle for staying abreast of risk balance as the implementation encounters (the inevitable) obstacles and surprises
    - Incorporates range of information: from educated guesses to detailed probabilistic assessments
  - Helps achieve 'optimally balanced' risk consistent with project resource constraints
  - Utilizes an underlying database which keeps growing
    - FMs, PACTs, and effectiveness: Part of ongoing FDPP Program
    - Previous evaluations
  - Provides explicit, traceable rationale for the inclusion (or exclusion) of various PACTs and risk elements

Current work and future plans

- Applications:
  - Technology road-mapping:
    - Ongoing at JPL, NEPP pilot at GSFC upcoming
  - Project Implementation:
    - Code Q budget for pilot applications
    - NASA Design for Safety Program (DfS)?
  - Mission and System Design:
    - Code Q budget for pilot applications
    - JPL CSMAD teaming, NASA DfS?
  - Technology Portfolios:
    - Teaming arrangements in development (NASA Code S, NASA DfS, DoD, JPL/TAP)
- Tool Availability:
  - Tool “official” releases every 6 months
  - Readily available to personnel for performing NASA work

DDP Tool Development

		Database/Fields	Impacts/Effectiveness	Computation	GUI
DDP 2.0		Underlying dbf holds variety of field entries and version control	Impacts scored via (and, or, push down or pull up), user defined functions[1]	Sums, products, functions, user defined functions [1]	Matrix views, column/row view, 'bouncing ball', user input view, RBP view, color-coded risks, variety of adjustable parameters
Next		Configuration Management	User defined functional relationship, logical relationship creator	Optimizer, arbitrary user functions	As requested by users

		User	Reporting	Interfaces	Population
DDP 2.0		Help, roadmap, user identification [1], partial class creation/instantiation	Variety of selectable reports with trees and bar graphs	Import/export data with Excel	PACTs for traditional space flight qualification, Generic FMs and FMs/PACTs for specific component types
Next		User identification and Configuration Management, Simultaneous interacting users, full class creation/instantiation, additional 'wizards'	Export directly into a Word Processing window	Import/export schedules, logical relationships (e.g. DOORS, Fault Trees), Export graphics to Excel	Continue to expand PACT suite, update effectivenesses and FM classes with current data, add additional technology types, etc.

[1] Currently available only in the java version of DDP

What you can do next

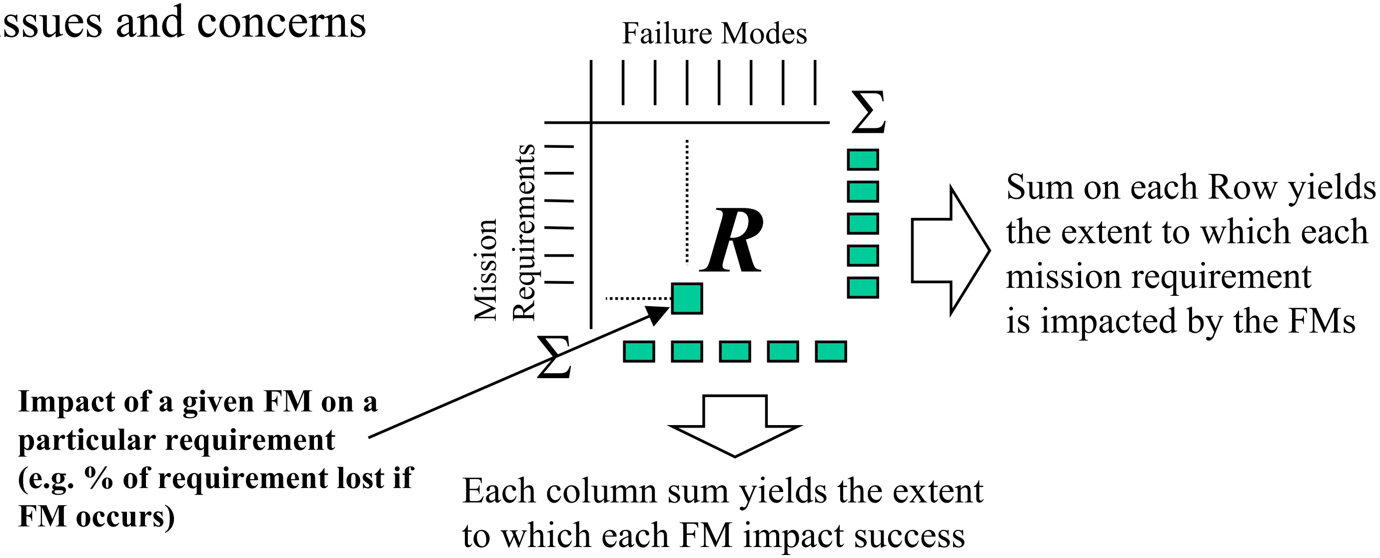
- Ignore all of this (I really hope not!)
- Get additional information/education
  - Schedule a tutorial, synchronize with a visit out this way
  - Get a copy of the tool (**Contact Steve Botzum@GSFC**)
  - Watch for upcoming website
- Try it on your project
  - We can help facilitate initial usage on a few projects over the next several years
    - Tutorials and/or detailed discussions
    - Provide facilitator and/or team members
- Contact Information:
  - Dr. Steven Cornford: (818)354-1701, steven.cornford@jpl.nasa.gov

  OR
  - Mr. Timothy Larson: (818)354-0100, timothy.larson@jpl.nasa.gov

BACK-UP SLIDES

Step 1: Develop the Requirements Matrix

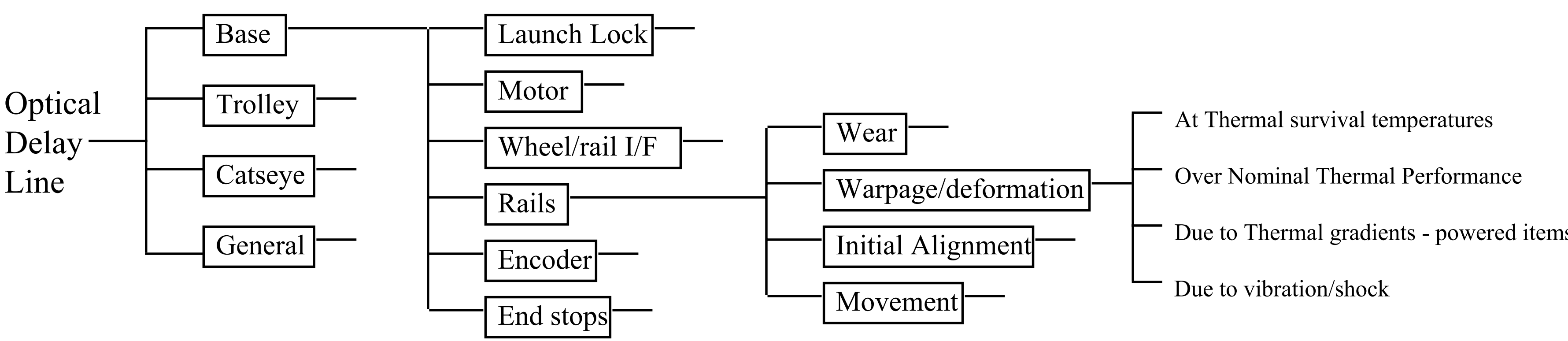
- Where are we going, what are we doing there, and for how long are we doing it? - Prioritize issues and concerns



- **Identify requirements**
  - Weight by importance to project
  - Will result in an indentured list
  - Can get information from project personnel or requirements documents
- **Identify failure modes**
  - May have non-certain likelihood of occurring if we do nothing
  - Will result in an indentured list
  - From FMECA, brainstorming, FTA, experience, etc.
- **Evaluate impacts of FMs (if occurs) on requirements**
  - Use percentage of requirement lost
  - Start with: 0, 0.1, 0.3, 0.9 and 1.0, refine with better numbers as get more detailed

Identifying the Failure Modes/Risk Elements

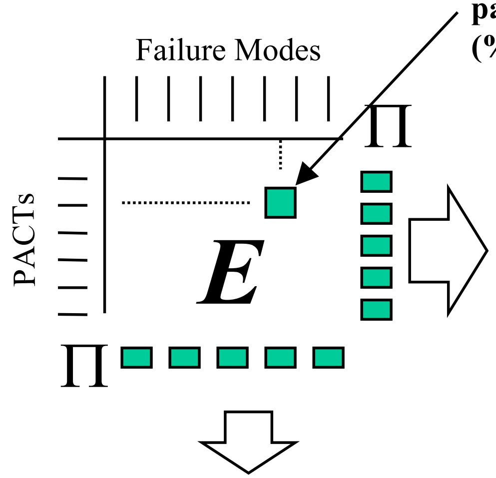
- **First step: Understand the system or technology**
  - Drawings/schematics, block diagrams, functional requirements, WBS elements, etc.
- **Failure Mode Identification Methods**
  - Brainstorming with "critical mass" of expertise of designers and specialists
  - CogE/expert interviews
  - Use requirements to help ID failure modes
    - What could keep requirement from being met?
  - Integrate Top-down and bottom-up evaluations
  - Integrate results/information from other tools and processes
    - Fault Trees, Risk Models, Requirement trees, etc.
  - Produces a failure mode/risk element tree



Step 2: Develop the Effectiveness Matrix

- How do we adequately ensure success in the presence of potentially activated failure modes and defects?

Effectiveness of a given PACT* on a particular FM (% chance of detecting or preventing)



Product of elements within a Row yields, ***f***, figure of merit for each PACT*

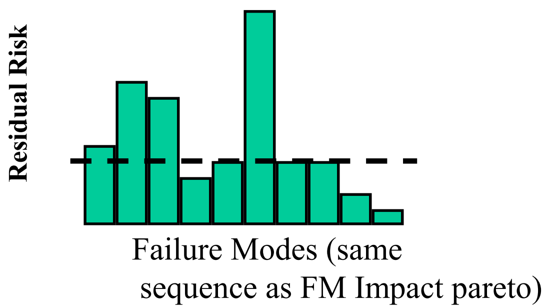
Product of elements within each Column yields ***e***, the net PACT* coverage for each failure mode ("Escape" chance)

- **Utilize failure modes identified in previous step**
- **Identify PACT* options**
  - We will have a 'pre-canned' set
  - Include efforts designers have put into clever designs which prevent problems from occurring
- **Evaluate effectiveness of PACTs on detecting/preventing failure modes**
  - Start with: 0, 0.1, 0.3, 0.9 and 1.0, refine with better numbers as get more detailed
  - ***PACT**s = **P**reventative measures, **A**nalyses, process **C**ontrols, and **T**ests
    (i.e. everything we can do to detect/prevent failure modes)

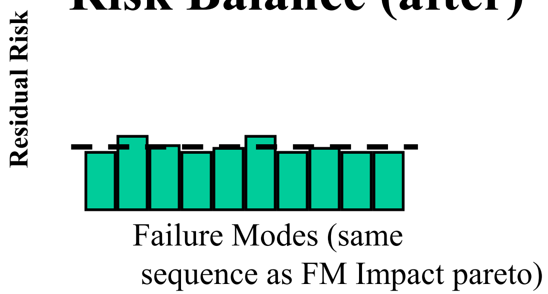
Step3: Using DDP to Tailor and Optimize

- Risk Balance
  - The residual risk is the 'expected value' of the failure mode, i.e, the product of it's likelihood, severity and chance of escaping
  - Measures product of how much we care and chance we will miss it
- Risk balancing trades off PACT options against residual risks
  - Versus constraints (mass, power, $, etc.)
  - Can shift priorities
  - Select different PACT combinations
  - Capture design and PACT decisions
  - Modified/refined with project life cycle

Risk Balance (before)



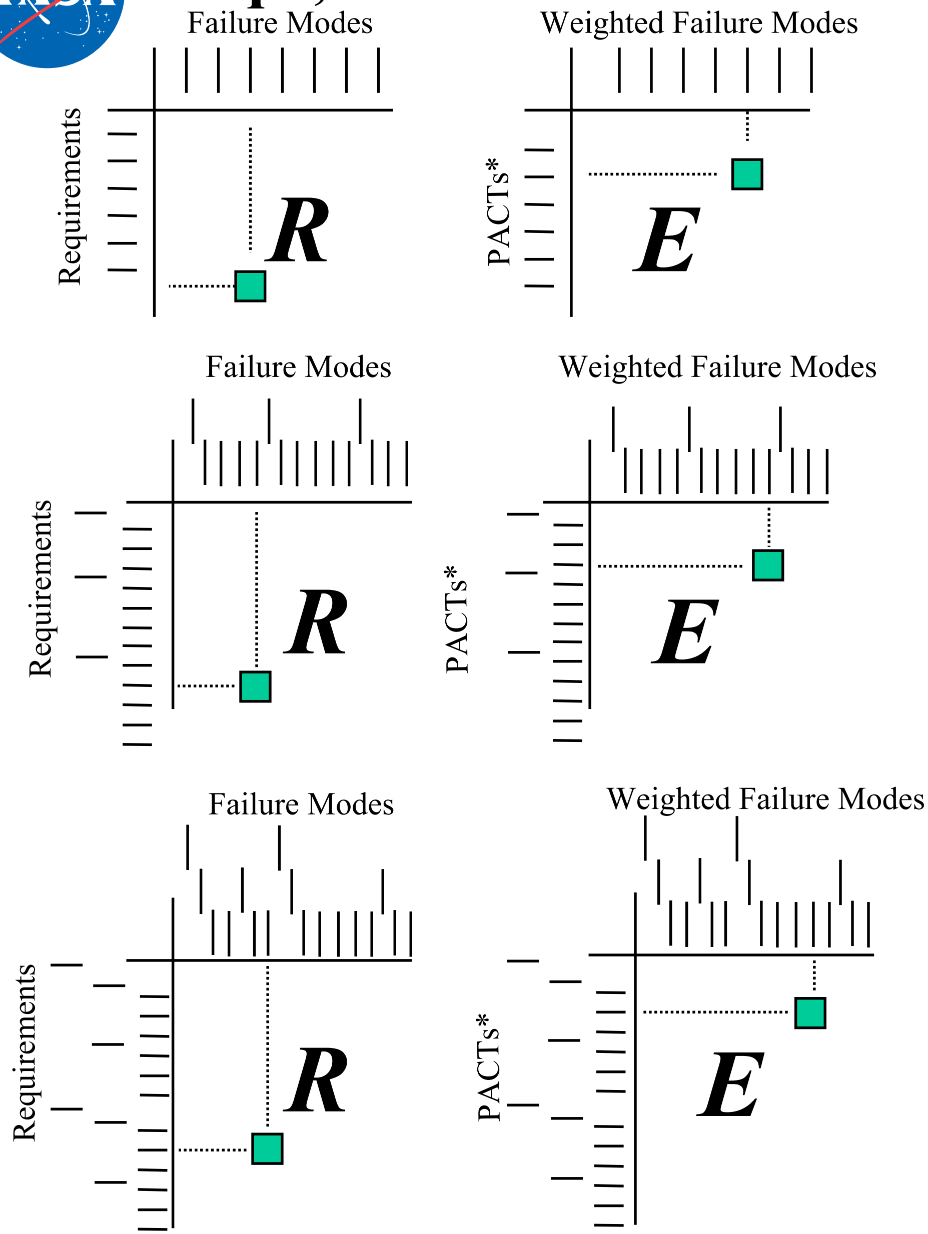
Risk Balance (after)



For each failure mode:

Residual Risk = r = i x e =The extent of it's impact x How likely it will occur

Reqts, FMs and PACTs are iteratively refined



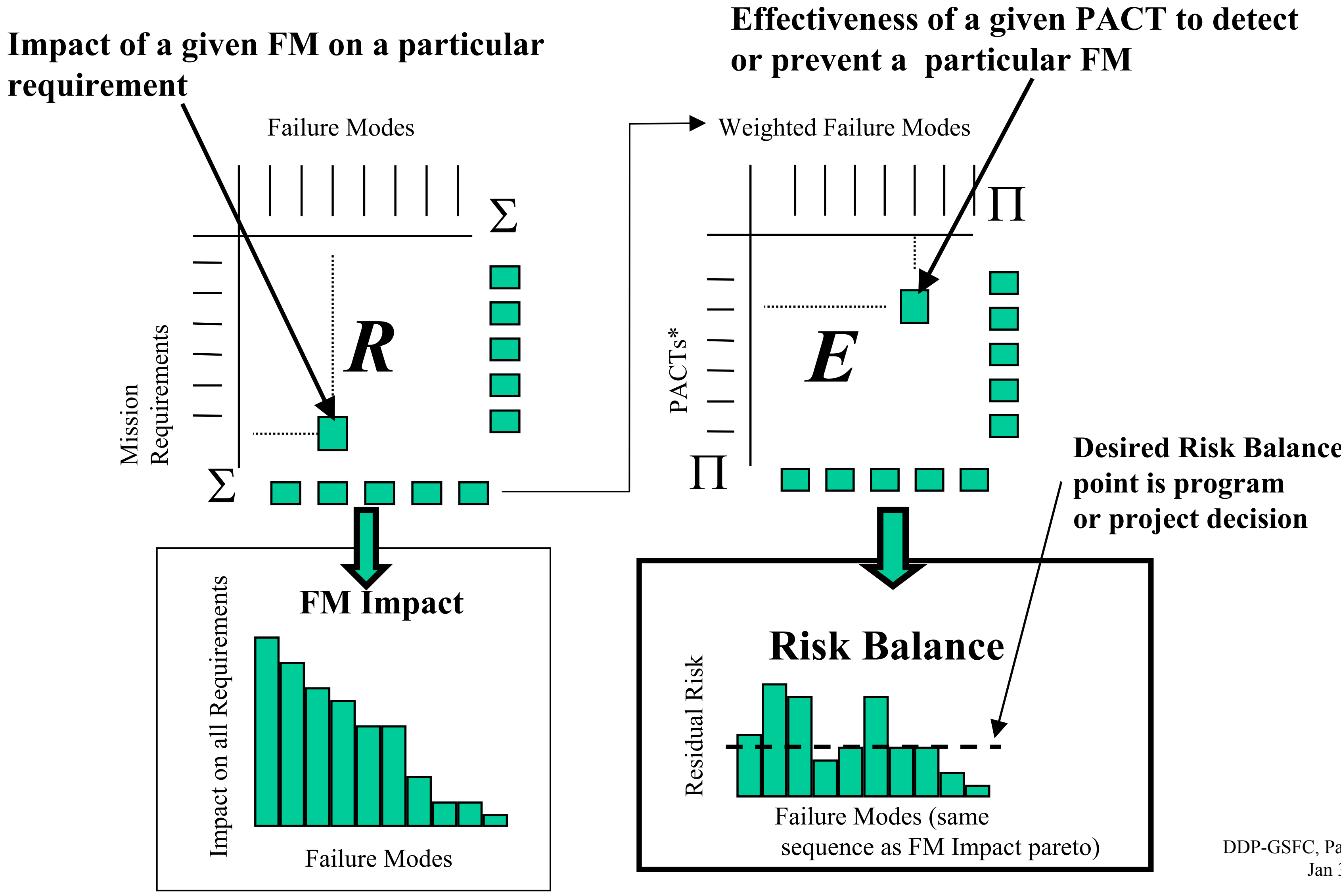
- Begin with high level
  - Mission requirements, failure mode and PACT categories
  - Matrix entries may represent mostly engineering judgement
- Refine to lower-levels
  - System requirements, lower-level failure mode and PACT categories
  - Matrix entries rely less on judgement and more on underlying physics or engineering
- Continue to refine as needed
  - Focus on areas identified as highest risk/uncertainty
  - Box-level requirements, failure mode and PACT types
  - Matrix entries may now mostly be based on historical data, focused evaluations, research findings, performance testing, etc.

Some Computational Details

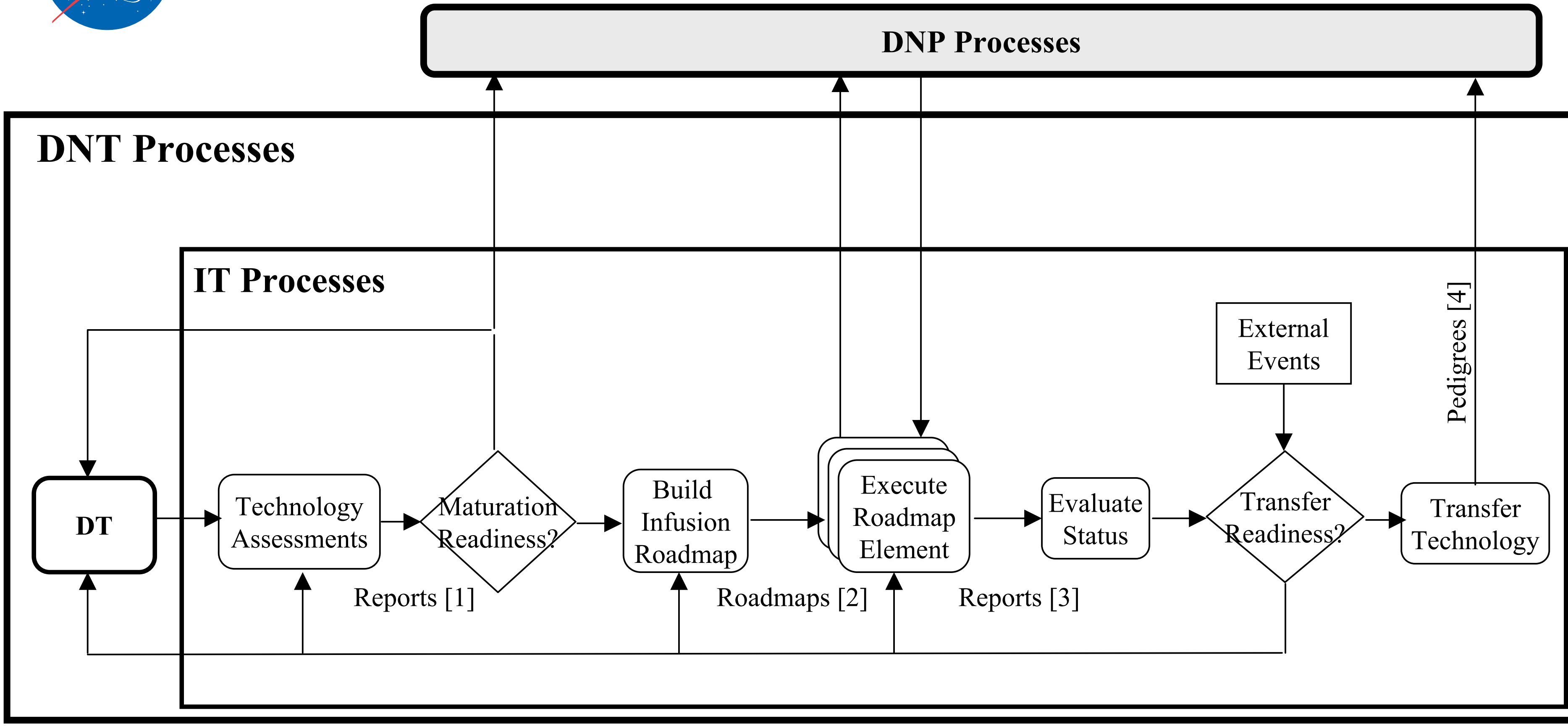
- Use best available information in filling out the matrix
  - Use applicable historical data, modeling, simulation or test results, or focused evaluation efforts
  - Begin 1, 3, 9 “engineering judgement scale” from Quality Functional Deployment - More typical at higher levels of evaluation
    - 0, 0.1, 0.3 and 0.9 are fractions of requirement not met
    - or 0, 0.1, 0.3, 0.9 are chance of detection/prevention by a PACT
- Use more detail as knowledge or need warrants - Typically at lower levels
  - Advantage of Physics of Failure approach is that we can leverage the volumes of data in industry and universities
  - May know particular requirements response or specific PACT effectiveness
  - FM likelihoods may be available from statistical models, vendor data, historical data, focused R&D efforts including technology development
- Areas of uncertainty can be flagged as liens which may go away if other PACTs are found effective or impact is evaluated in detail
- Risk Balance
  - Can be simple product I just described or more sophisticated functional relationships

Simplified DDP Summary

• DDP utilizes two matrices: the Requirements matrix (***R***) and the Effectiveness matrix (***E***)



Process chart for Infuse Technology (IT)



XXX = Other DNT Processes XXX = IT sub-processes

[1] These reports include the results of the various assessments including risk and maturity evaluations, and the information necessary to build infusion roadmaps

[2] These roadmaps include technical milestones, optimal risk reduction paths, success criteria and critical documents/records

[3] These reports include the results of element execution and measurements of progress against the roadmaps

[4] Pedigrees include results and recommendations, but may also include hardware and software components

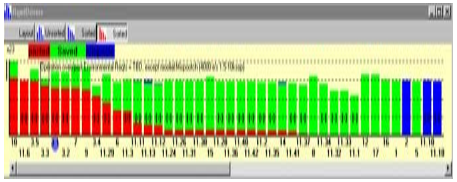
Tools for Managing Infusion Risk

•Have developed and applied a tool for assessing the maturity of technologies and roadmapping the path to infusion

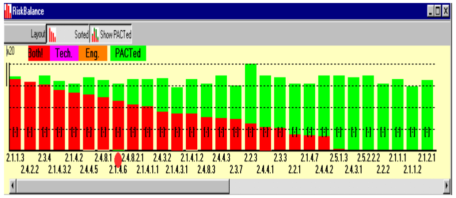
•Determine the relative importance of various risk elements
- •Input trees of requirements (and relative importance)
- •Input trees of risk elements
- •Evaluate consequence (and likelihood) of risk elements on each requirements

•Select PACT combinations to reduce risk (**P**reventative measures, **A**nalyses, process **C**ontrols and **T**ests)
- •Use existing database or add new ones
- •Each has an effectiveness at detecting (or preventing) the occurrence of some collection of risk elements
- •Each has resource costs associated with it ($, schedule, mass, etc.)
- •Choose a combination of PACTs

•Results: Requirements drivers (extent to which requirement is/was at risk)
- •Total height indicates extent to which requirement was at risk (really needed?)
- •Red indicates extent to which requirement is still at risk (need to do more?)
- •Blue are requirements not at risk (do they belong?)

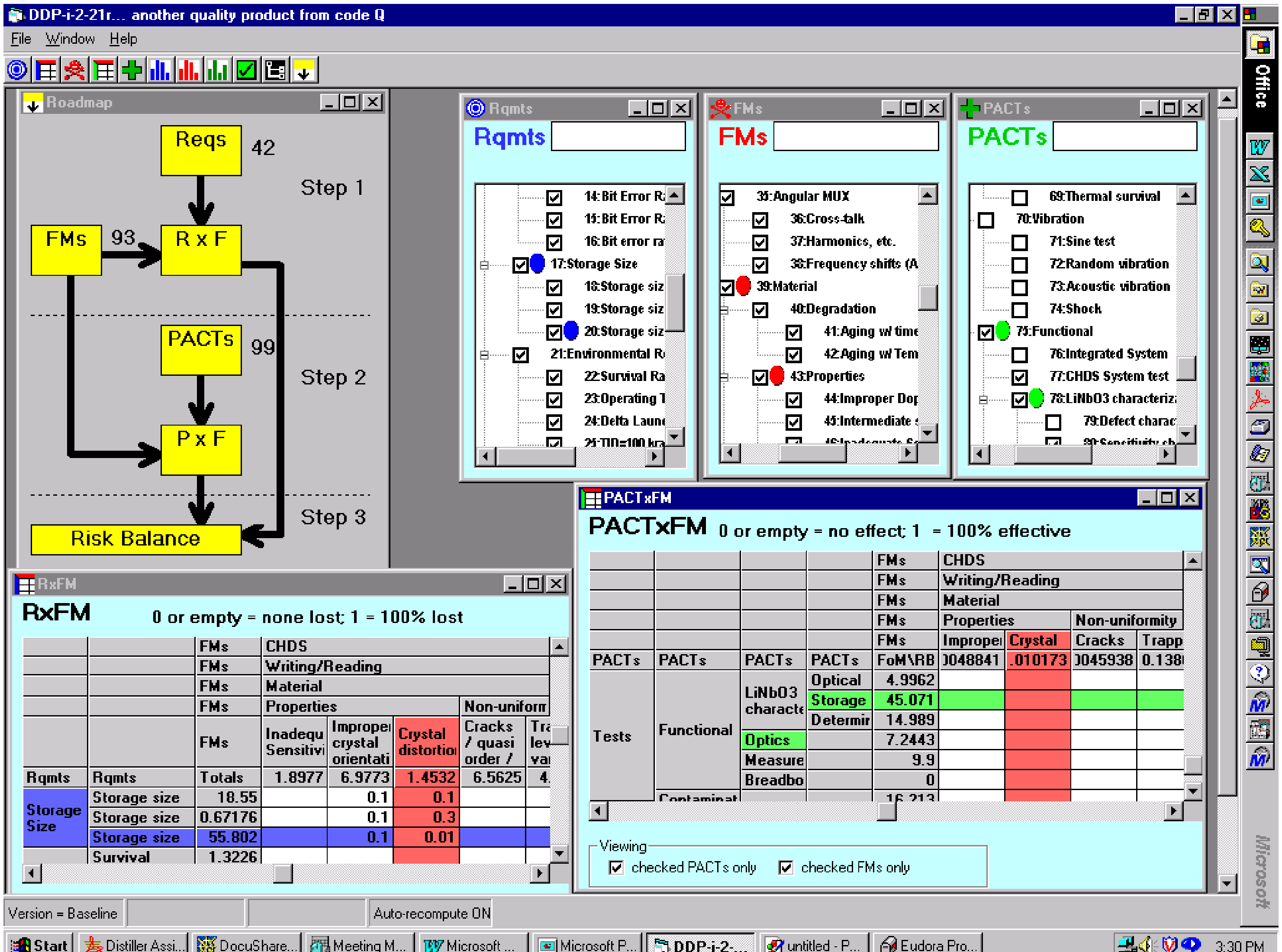


•Results: Residual Risk (extent to which a risk element is still present)
- •Total height indicates relative criticality of each risk element
- •Green indicates extent to which each element which has been eliminated
- •Red indicates extent of residual risk of each element



•Results: PACT combination selected for implementation
- •Begin detailed WPA development
- •Each now has specific, traceable reasons for implementation
  - •Enables improved tailoring
  - •Enables decisions regarding consequences of not doing

Backup


DDP-i-2-21r... another quality product from code Q
File Window Help
Roadmap
Reqs
42
Step 1
FMs
93
R x F
PACTs
99
Step 2
P x F
Step 3
Risk Balance
Rqmts
FMs
PACTs
14:Bit Error R
15:Bit Error R
16:Bit error ra
17:Storage Size
18:Storage siz
19:Storage siz
20:Storage siz
21:Environmental R
22:Survival Ra
23:Operating T
24:Delta Laune
35:Angular MUX
36:Cross-talk
37:Harmonics, etc.
38:Frequency shifts (A
39:Material
40:Degradation
41:Aging w/ time
42:Aging w/ Tem
43:Properties
44:Improper Dop
45:Intermediate
69:Thermal survival
70:Vibration
71:Sine test
72:Random vibration
73:Acoustic vibration
74:Shock
75:Functional
76:Integrated System
77:CHDS System test
78:LiNbO3 characteriz
79:Defect charac
RxFM
0 or empty = none lost; 1 = 100% lost
PACTxFM
0 or empty = no effect; 1 = 100% effective
FMs CHDS
FMs Writing/Reading
FMs Material
FMs Properties Non-uniform
Inadequ Sensitivi
Imprope crystal orientati
Crystal distortio
Cracks / quasi order /
Rqmts Rqmts Totals 1.8977 6.9773 1.4532 6.5625
Storage Size
Storage size 18.55 0.1 0.1
Storage size 0.67176 0.1 0.3
Storage size 55.802 0.1 0.01
Survival 1.3226
Non-uniformity
Crystal Cracks Trapp
PACTs PACTs PACTs PACTs FoM\RB
Tests Functional
LiNbO3 characte
Optical 4.9962
Storage 45.071
Determir 14.989
Optics 7.2443
Measure 9.9
Breadbo 0
Viewing
checked PACTs only
checked FMs only
Version = Baseline
Auto-recompute ON
Start
3:30 PM